The Privacy Paradox - Investigating People's Attitude Towards Privacy in a Time of COVID-19

R. Trestian[1], E. Celeste[2], G. Xie[2], P. Lohar[2], M. Bendechache[2], R. Brennan[2], I. Tal[2]

[1]Middlesex University, London, UK
{r.trestian}@mdx.ac.uk

[2] Dublin City University, Dublin, Ireland
{guodong.xie, pintu.lohar}@adaptcentre.ie, {edoardo.celeste, malika.bendechache, rob.brennan, irina.tal}@dcu.ie

***Abstract*—The advent of digital technologies used as a mechanism to deal with the Covid-19 global pandemic, has raised serious concerns around privacy and security issues. Despite these concerns and the potential risk of data misuse, including third party use, countries around the world have pushed the use and proliferation of contact-tracing applications. However, the success of these contact-tracing applications relies on their adoption and use. A well known phenomenon referred to as privacy paradox is defined as the discrepancy between the expressed privacy concern and the actual behaviour of users when it comes to protect their privacy. In this context, this paper presents a study investigating the privacy paradox in the context of a global pandemic. A national survey has been conducted and the data is analysed to examine people's privacy risk perception. The results show inconsistencies between people's privacy concerns and their actual behaviour that is reflected in their attitude shift of sharing their mobile data during a global pandemic. The study also compiles a list of recommendations for policymakers.**

***Index Terms*—privacy paradox, contact tracing, data privacy, Covid-19**

I. Introduction

The significant advancements in technology over the past several years have led to the proliferation of powerful and affordable mobile device. However, the increase in the adoption of mobile devices has also seen an increase in the cyber attacks and data breaches. Thus, exposing the mobile users to security and privacy threats. Additionally, studies have shown that within this digital age the main concern for the mobile users is their data privacy [1]. However, even after high profile incidents of unauthorized access and abuse of personal information like the case of Facebook and Cambridge Analytica [2], mobile users still lack in properly managing their privacy settings. This inconsistency between the mobile users' privacy concerns and their actual behaviour towards privacy is known as the *privacy paradox*. Previous studies have shown that in general, the mobile privacy concerns and the trust of the mobile platform are among the main determinants of attitude towards information sharing [3].

Figure 1(a) illustrates the general conceptual model of disclosure which shows that the *risk* defined as the perceived disclosure consequences and *trust* influence directly the behavioural intentions that would then influence the actual disclosure behaviour. However, Norberg et al. [4] argued this theory and proposed the privacy paradox conceptual model illustrated in Figure 1(b) which considers the risk only influencing the behavioural intention to disclose, while trust will impact the actual disclosure behaviour.

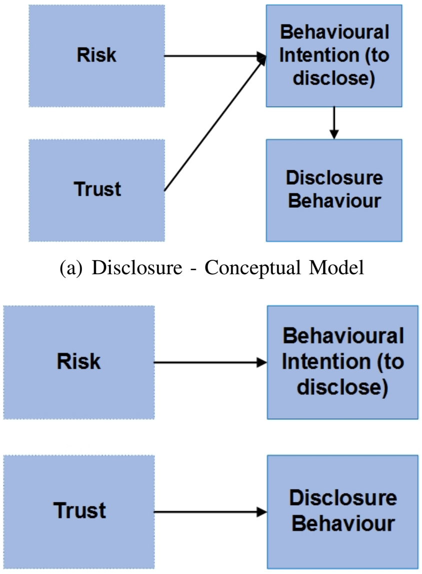
Risk
Behavioural Intention (to disclose)
Trust
Disclosure Behaviour
(a) Disclosure - Conceptual Model
Risk
Behavioural Intention (to disclose)
Trust
Disclosure Behaviour
(b) Privacy Paradox - Conceptual Model

Fig. 1: Disclosure vs. Privacy Paradox Conceptual Models

Consequently, when the global Covid-19 pandemic measures seen an increase in the use of pre-existing digital technology tools as well as new digital solutions to help at maximising the containment measures and stop the spread of the virus, it also led to an increase in the already existing privacy concerns. This is because most of the digital tools introduced to limit the spread of the virus, significantly interfere with our digital traces by processing sensitive personal information [5]. However, one cannot underestimate the risks that the misuse of digital technologies may have on the citizens' fundamental rights, particularly on the rights to privacy and data protection.

In this context, this paper aims to assess the privacy paradox in the context of the global pandemic and analyse whether the use of digital technology tools to fight the pandemic has also been accompanied by a change of attitude regarding privacy and data protection preferences. The starting hypothesis was that, in general, the adoption of digital technology tools that might be more privacy intrusive and riskier from a data protection perspective is also accompanied by a major complacency of the population. Our initial pilot survey conducted on a 258 participants sample [6] showed that people are willing to share their personal data in the interest of controlling the spread of the virus and save lives.

In this paper, we have extended the pilot study to a national survey reaching a sample of more than one thousand residents of Ireland. The results of the national survey confirm the results of the pilot study and showed that people had effectively changed their privacy attitudes in light of the global Covid-19 pandemic, but that a significant portion did not trust the technological tools introduced by the government, despite their formal legality.

II. Digital Technologies to Fight Covid-19

In order to curb the spread and intensity of the Covid-19 pandemic, countries around the world turned to the use of digital technologies. Different digital technologies have been used for different purposes, such as: contact tracing, symptom checking, quarantine enforcement, mobility monitoring, etc.

One of the most popular approach in the use of digital technologies as response to Covid-19 pandemic is the adoption of contact tracing mobile applications. Contact tracing deals with the identification and notification of someone's *close contacts* considered to be at risk of developing or carrying Covid-19 due to being within the distance and within a time frame considered necessary for transmission to have occurred. A detailed review of these Covid-19 contact tracing apps is presented in [7]. These approaches can be mainly classified in centralized and decentralized [8] approaches and they predominantly rely on Bluetooth, GPS, QR codes, and cellular location tracking [9]. The decentralized approaches store and process data in a decentralized manner, meaning that the data is stored locally on the user's device. In contrast, the centralized approaches controversially process the users data on a centralized server, meaning that data leaves the user's device. This second approach is considered to be less privacy preserving, less compliant with the data minimization and purpose limitation principles more likely to lead to re-identification, and more likely to be at risk of hacking.

The contact tracing apps that use the GPS location tracking will track users' location in order to establish their contacts. Some examples of such apps are: *Private Kit: Safe Paths* in United States), *Corona 100m (Co100) App* in South Korea, *Hamagen App* in Israel, *PeduliLindungi* in Indonesia, *AOT Airports, PedKeeper, ThaiChana,* and *MorChana* in Thailand. The use of GPS location tracking has been extremely common in China where apps are used in particular regions that impose varying levels of restrictions based on a colour-coded, green/yellow/red, scale of users' health status, and where telecommunications providers may provide location data to authorities. These uses do not seek the consent of individuals and often lack transparency.

Proximity data through Bluetooth Low Energy (BLE) has also been adopted by several contact tracing apps, including: *NHS Covid-19 App* in United Kingdom, *TraceTogether* in Singapore, *Stopp Corona* in Austria, *Immuni* in Italy, *CovidSafe* in Australia, *Corona-Warn-App* in Germany, and *ProteGO Safe* in Poland. These apps based on BLE do not track users' location, but rather are programmed to establish a connection when the device has been within the proximity and for the amount of time that is considered to establish someone as a *close contact* for the risk of Covid-19 transmission [10].

Apart from contact tracing apps, symptom checking apps have also been used for the main purpose of symptom checking and monitoring, both for those with and without a Covid-19 diagnosis. These include apps produced as part of a governmental response, such as the United Kingdom's *Covid Symptom Tracker* and Spain's *StopCovid19Cat* which enable users to report their own symptoms. In Germany the *Corona-Datenspende* app was used for the users to initially enter their data and the app then connects to other devices such as smartwatches or fitness trackers to record indicators of infection such as an increased heart rate or altered sleep pattern for the purpose of tracking the spread of Covid-19. Some of these apps have been made mandatory by states, such as Thailand's *DDC-Care* app through which users upload a self-assessment report. This was made compulsory for those with a Covid-19 diagnosis or who have travelled from contagious areas.

Other enabling technologies, such as drones using cameras and Artificial Intelligence (AI) have been used for example in Australia, to measure heart and respiratory rates for fever detection and symptom checking. In Russia, cameras using facial recognition techniques were used to ensure those ordered to quarantine were complying. Apps that track health status, travel history, location and contacts in order to code people as Green/Yellow/Red depending on diagnosis or risk of exposure have been employed by Chinese authorities [11].

A. Privacy Implications

All digital technology tools that have been introduced to limit the spread of Covid-19 have data privacy and protection implications. Firstly, they all rely on the processing of data related to identifiable individuals in order to achieve their purposes. Secondly, they process information related to aspects of the citizens personal and family lives, such as social interactions, movements and health status. The adoption of these technologies is legitimate as far as data protection principles are respected and the intrusion into the citizens personal and family life is justified, necessary and proportionate to the purpose of solving a global health crisis. However, in some cases the use of digital technology tools to limit the spread of Covid-19 has produced a series of violations of these fundamental rights.

The most concerning scenario is offered by undemocratic states where government authorities carried out a systematic monitoring of location, travel history and contacts between persons, using the fight against Covid-19 as a reason to justify the implementation of mass surveillance measures. An apparent example is provided by the indiscriminate use by the Chinese government of the data collected by the Health Code apps [11]. However, studies [12] have observed that measures implemented to halt Covid-19 also emerge as extensions of already ongoing moves to engage in domestic surveillance. This appears to be the case in Israel where the government has employed legal mechanisms intended for counter terrorism purposes in order to use its security services to harness and utilize location and contact data for contact tracing and to serve isolation orders. In any case, as stated by the European Data Protection Board, the use of digital technologies adopted to limit the spread of the virus for mass surveillance purposes represents a 'grave intrusion into people's privacy' and illustrates the risk of mission creep of the use of technology in combating the pandemic.

Consequently, one common fear is that the personal data collected by the contact tracing apps could be used indefinitely beyond the end of the pandemic and the surveillance opportunities enabled by these apps will not be abandoned by the governments [12]. These concerns are not unfounded, considering that the surveillance measures implemented in the US in the wake of 9/11 still remain in place today. While in the United Kingdom there are plans in place to retain the collected data for up to 20 years while the individuals absolute right to have their data deleted upon request is denied [12].

III. Privacy Paradox during Covid-19

This paper presents a study based on a conventional questionnaire that is distributed online with the aim to investigate and report on the attitudes to privacy of the residents of Ireland during COVID-19 times. An initial overview of the survey's results was presented in [8] where we looked at the citizens willingness to share their personal data as well as the formal legality versus the legal reality.

In this paper we are going to analyze the main factors that are involved in the privacy paradox conceptual model, such as risk and trust.

A. Survey Details

The survey is structured in three parts: (1) demographics - collects demographic data based on the guidelines in [13]; (2) privacy profiles - builds general privacy profiles based on the Privacy Segmentation Index (PSI) [14] that classifies individuals into three groups: privacy fundamentalists, pragmatics, and unconcerned; and (3) privacy attitudes during Covid - includes questions related to sharing personal data in the interest of saving lives, usage of the Covid tracker app, and also questions that relate to possible factors that have an impact on the attitudes (e.g. the concern of getting infected with Covid-19) with the aim to capture the citizens' attitudes toward privacy in Covid-19 times.

The national survey has been conducted online during November 2020 to January 2021 and was targeted at the Irish population over 18 years of age. The survey collected 1001 effective responses from 1012 participants, while 11 incomplete responses were discarded. Of all participants, 489 are identified as male and 490 as female, 4 as non-binary and 18 choose not to say. 503 of all the participants, accounting for 50% are within the 25 to 44 years old age group.

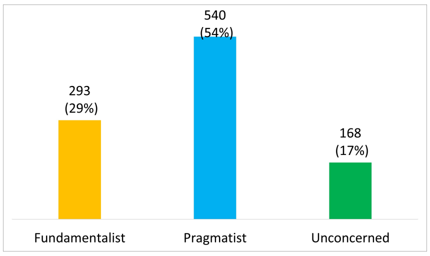

Fig. 2: Privacy Classification - Survey Results

B. Privacy Profiles

To understand the general privacy profiles of the participants based on the PSI defined by Westin, [14] the following three statements were presented to the participants and they were asked to rate them between *Strongly Disagree* and *Strongly Agree* on a four-point scale:

1) Consumers have lost all control over how personal information is collected and used by companies.
2) Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Following their responses to these three statements, the participants are classified into three categories: (1) *privacy fundamentalists* are the most privacy-oriented and concerned and they agree with statement 1) and disagree with statement 2) and 3); (2) *privacy unconcerned* are not at all privacy-oriented and they disagree with statement 1) and agree with statements 2) and 3); and (3) *privacy pragmatists* are the remaining participants that are in between the other two categories. The classification results of the participants in the national survey are presented in Figure 2. It can be noted that the majority of the participants are privacy pragmatists, which is in line with the results of previous Westin's studies [14] as well as our pilot study [6].

C. Risk Attitude

A *risk score* was computed to determine the general level of concern when sharing personal data via the mobile apps installed on the mobile devices. The following four statements have been used to compute the *risk score* by allocating points to the responses and taking the average [15].

1) I feel safe giving mobile apps access to my personal data and device tools.
2) Providing mobile apps with access to personal data and device tools involves too many unexpected problems.
3) I generally trust mobile apps with handling my personal data and device tools.
4) How concerned are you about threats to your personal privacy when using mobile apps.

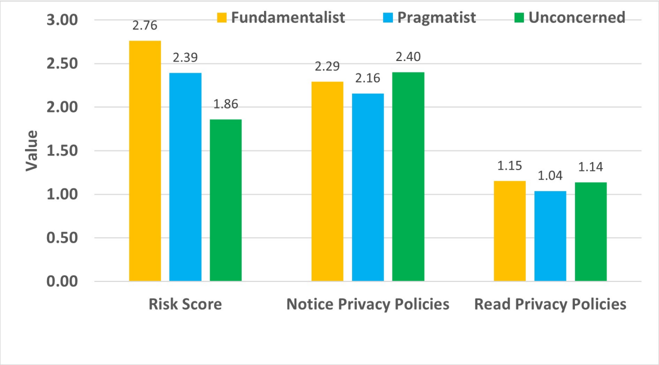

Fig. 3: Risk Attitude - Survey Results

A high *risk score* value means a greater feeling of concern or perceived risk in relation to using mobile apps. The following two additional questions were used to analyse the general privacy attitudes of the participants:

1) Do you generally notice whether or not a mobile app you want to install on your phone has a privacy policy?
2) How often do you read mobile apps' privacy policies?

Figure 3 illustrates the risk attitudes results grouped as per Westin's classification. As expected, the results indicate that the privacy fundamentalists have a greater feeling of concern or perceived risk when it comes to sharing their personal information using the mobile apps. However, there are no unusually high levels of risk perceived by the three categories. While all three categories have a similar approach of not reading the privacy policies very often and noticing the privacy policies on average.

D. Trust Attitude

Participants were also asked what kind of mobile data and with which institutions they would be willing to share their data in the context of Covid-19 outbreak. More than 50% of the participants would agree to share their anonymized mobile geolocation data and the health status data. When asked about specific organizations or sectors with whom the participants would agree to share their mobile data, the top organizations were: public health authorities (859 respondents), Government (482 respondents), Public apps sharing anonymized data (366 respondents), Private/commercial apps sharing anonymized data (147 respondents), private health companies/agencies (105 respondents).

Responses to the question *Would you be concerned in relation to how your personal data would be used by the government and relevant institutions in order to defeat Covid-19?* demonstrated that when facing Covid-19 most respondents tend to not be too concerned about how their personal data are used by the government (*Not concerned at all* and *Slightly Concerned* accounts for 46% of respondents). However, 31% of the participants would be moderately to extremely concerned and the top concerns are listed in Table I.

TABLE I: Factors of concern for sharing the mobile data

Are the concerns related to:	**Counts**
Privacy issues	582
Lack of trust in the Government and the institutions managing the data	483
Security issues	469
creating dangerous precedent	418
Other	30

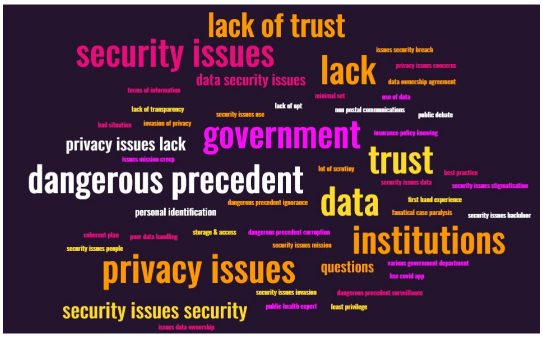

Fig. 4: Trust Attitude Word Cloud - Survey Results

The specific concerns were captured in a word cloud illustrated in Figure 4. The words larger in size are the most frequent terms in the responses, such as: lack of trust, trust, government, privacy issues, etc. Consequently, the data shows that the Irish residents uphold a significant mistrust in the public and private institutions overseeing the global Covid-19 health crisis.

E. Privacy Paradox in a Time of Covid-19

To study the privacy paradox in terms of the inconsistency between the privacy concerns of the participants and their actual behaviour towards privacy, we analyze if their attitude towards willingness to share their data under normal circumstances has changed as compared to during Covid-19 outbreak. In doing this, we look at the participant's responses to the following two questions:

1) Would you agree to share your mobile data (data stored or related to your mobile device) to help defeat Covid-19? *(Strongly disagree, Disagree, Neutral, Agree, Strongly agree)*
2) Would you agree to share your mobile data with the above institutions/organizations in normal circumstances (not during a public health crisis)? *(Strongly disagree, Disagree, Neutral, Agree, Strongly agree)*

The results are illustrated in Figure 5 as per Westin's classification.

As expected, the highest shift in attitude is recorded by the privacy *Unconcerned* category with a jump from 23% before the pandemic to 80% during the pandemic, that *Agree* and *Strongly agree* to share their mobile data. The most surprising attitude shift comes from the privacy *Fundamentalist* with a jump from 7% before the pandemic to 53% during the pandemic (*Agree* and *Strongly agree*). This attitude shift is surprising because privacy *Fundamentalist* people are the most protective of their privacy being described as supporting stronger laws to safeguard an individual's privacy. Thus, this behaviour can be explained as the privacy paradox.

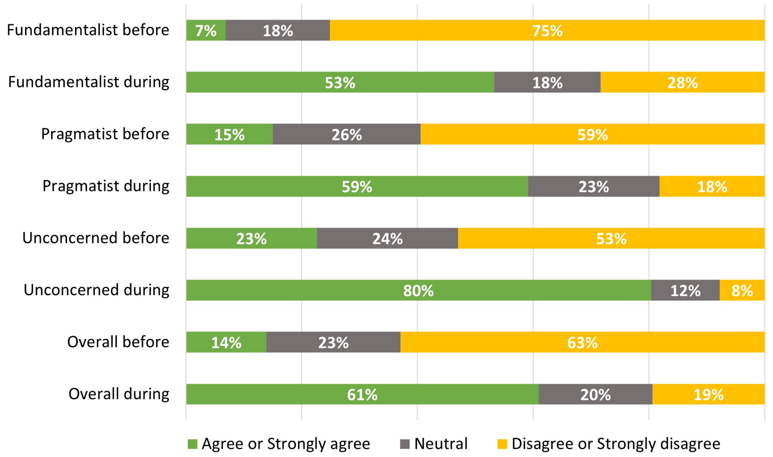

Fig. 5: Privacy Paradox - Willingness to share personal data before and during Covid-19

TABLE II: Use of Digital Technologies for Covid-19

Digital tracking technologies are important to help control COVID-19 spread and monitor public health	**Counts**
I would use these technologies, but have concerns about ensuring the regulatory policies or specifications	335
I would use these technologies	269
I would not use these technologies as I feel there is a lack of ethics and regulatory specifications	28
I would not use these technologies as they are the gateway to extended surveillance (after COVID-19 situation)	27
I would not use these technologies because I fear they would share my data with private companies	24
I would not use these technologies as they are an invasion of privacy /there is no guarantee for data protection	19

F. Digital Technologies and Covid-19

When asked *Do you agree with the statement "Digital tracking technologies are important to help control COVID-19 spread and monitor public health" (Strongly disagree, Disagree, Neutral, Agree, Strongly agree)*, 40% of participants choose *Agree* or *Strongly Agree*. Thus, regardless of their attitude shift during pandemic, these results indicate that 40% of participants believe that digital tracking technologies are helpful to help control the pandemic. For these participants, most of them would use a digital technology solution like the contact tracing app. However, they would still have concerns about ensuring the regulatory policies and specifications, as indicated in Table II.

Moreover, 62% of the respondents have indicated that they were using the HSE COVID tracker application. However, even though they have decided to use the app, they still have concerns as indicated in Table III.

The results indicate that 30% of the participants that are using the Covid-19 tracker app, feared that the app could be used as a surveillance tool beyond its primary aim of fighting the spread of Covid-19 while 28% of respondents reported worries about the implications of using the app for their privacy and data protection. This data exposed a discrepancy between the formal legality and legal reality of the digital solutions adopted by the government. Indeed, the survey found that the Irish population perceives solutions employed to control the spread of Covid-19 to potentially infringe their fundamental rights, despite these solutions technically respecting the specific EU guidance and national law.

TABLE III: Concerns regarding the HSE COVID Tracker application

Regarding the HSE COVID Tracker application, select all the applicable statements below	**Counts**
I am worried that the application will be used as a tool of surveillance beyond the scope of COVID-19	168
I am worried about the implications this application will have on my privacy and data protection	163
I do not think the application is helpful in controlling the virus	125
I think the application is helpful in controlling the virus	103
I do not understand its utility	42
I like the application as it provides a good overview of the COVID-19 status in Ireland (for example up to date county stats, etc.)	37
I did not have a good user experience with the application (e.g. contact tracing was draining my battery, not user friendly, etc.).	27
I found the application easy to use	8
I already had COVID-19 and I consider the application is not relevant for me anymore	8
Overall, I had a good experience with the application	3

IV. Recommendations to Policymakers

As an outcome of the study presented above, a series of recommendations for policymakers are listed below:

A. Transparency

Enhancing transparency and data protection literacy is of utmost importance. Adequate information should be provided to data subjects, even if legal bases other than consent for data processing are available. This information should be provided using clear and intelligible language in order to help improve the population's understanding of the norms and methods implemented by digital responses to Covid-19. This should be ensured with regards to the methods used and actors involved in digital responses to the Covid-19 crisis. Policymakers should be upfront about the challenges posed by the lack of knowledge and experience of events like the global Covid-19 pandemic, and that while governments and policymakers may be doing their best with the information available to make responsible choices for the entire population, sometimes responses might fail despite these good intentions.

B. Participation in decision making

In order to increase levels of literacy in the field of data protection and privacy, participation of the general population should be sought during decision making processes. This should aid in enhancing awareness in the population that privacy and data protection cannot be fully sacrificed. Involvement of the wider population in early phases of decision-making processes related to the employment of digital technology solutions to fight Covid-19 is crucial to enhance the level of legitimacy of the adopted solutions and as a trigger of greater transparency of the decision-making processes.

C. Public actors

A greater involvement of and reliance on public actors is recommended. The involvement of private actors for the sake of efficiency should be avoided, and in circumstances where they are used, how and why public and private actors are cooperating should be fully explained to minimise the discrepancy between formal legality and legal reality.

D. Data minimisation

To help and maintain a balance between public health and other interests, data should be processed in line with the data minimisation principle. Accordingly, only data necessary for contact tracing or other valid purposes should be collected, mission and function creep should be avoided, and the data should be deleted as soon as such a valid purpose expires. In particular, in relation to contact tracing, authorities should use proximity over geolocation data, reducing tracking or surveillance opportunities.

E. Voluntariness

Digital solutions to track and control the spread of Covid-19 should remain voluntary. Apps and other digital solutions should not be made mandatory by public or private actors, such as employers or airlines. In this way, our fundamental rights and freedoms, including the possibility of self-restricting them autonomously, remain protected.

V. Conclusions

This research presents the results of a national survey to study the privacy paradox during the Covid-19 pandemic. The use of digital technologies is of paramount importance when dealing with emergency responses such as the spread of the Covid-19. However, the adoption and the efficacy of the digital technology solutions are significantly impacted by the privacy and legal concerns around the use of personal data. The results indicate that there is some inconsistency between people privacy concerns and their actual behaviour reflected in their attitude shift of sharing their mobile data in the interest of controlling the spread of Covid-19.

Acknowledgements

This publication has emanated from research conducted with the financial support of Science Foundation Ireland through COVID Rapid Response programme grant number 20/COV/0229 and through the grant 13/RC/2094 co-funded under the European Regional Development Fund through the Southern and Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie) and the ADAPT Centre for Digital Content Technology (www.adaptcentre.ie) [grant number 13/RC/2106]. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

References

[1] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & security*, vol. 64, pp. 122–134, 2017.

[2] I. Kozlowska, "Facebook and data privacy in the age of cambridge analytica," *The Henry M. Jackson School of International Studies, Seatlle*, vol. 30, 2018.

[3] F. Bélanger and R. E. Crossler, "Dealing with digital traces: Understanding protective behaviors on mobile devices," *The Journal of Strategic Information Systems*, vol. 28, no. 1, pp. 34–49, 2019.

[4] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of consumer affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[5] B. d. A. Almeida, D. Doneda, M. Y. Ichihara, M. Barral-Netto, G. C. Matta, E. T. Rabello, F. C. Gouveia, and M. Barreto, "Personal data usage and privacy considerations in the covid-19 global pandemic," *Ciencia & saude coletiva*, vol. 25, pp. 2487–2492, 2020.

[6] R. Trestian, G. Xie, P. Lohar, E. Celeste, M. Bendechache, R. Brennan, and I. Tal, "Privatt-a closer look at people's data privacy attitudes in times of covid-19," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, 2021, pp. 174–179.

[7] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of covid-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134 577–134 601, 2020.

[8] R. Trestian, G. Xie, P. Lohar, E. Celeste, M. Bendechache, R. Brennan, E. Jayasekera, R. Connolly, and I. Tal, "Privacy in a time of covid-19: How concerned are you?" *IEEE Security & Privacy*, vol. 19, no. 5, pp. 26–35, 2021.

[9] J. Li and X. Guo, "Covid-19 contact-tracing apps: A survey on the global deployment and challenges," *arXiv preprint arXiv:2005.03599*, 2020.

[10] K. Riemer, R. Ciriello, S. Peter, and D. Schlagwein, "Digital contact-tracing adoption in the covid-19 pandemic: It governance for collective action at the societal level," *European Journal of Information Systems*, vol. 29, no. 6, pp. 731–745, 2020.

[11] E. Monaco, K. C. Tang, W. K. Cheng, H. Liu, and B. Pan, "Actions across government and covid-19: The experience of mainland china, macao and hong kong," in *COVID-19 Pandemic, Crisis Responses and the Changing World*. Springer, 2021, pp. 57–82.

[12] K. Eck and S. Hatz, "State surveillance and the covid-19 crisis," *Journal of Human Rights*, vol. 19, no. 5, pp. 603–612, 2020.

[13] J. L. Hughes, A. A. Camden, and T. Yangchen, "Rethinking and updating demographic questions: Guidance to improve descriptions of research samples," *Psi Chi Journal of Psychological Research*, vol. 21, no. 3, pp. 138–151, 2016.

[14] P. Kumaraguru and L. F. Cranor, "Privacy Indexes: A Survey of Westin's Studies," Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU-ISRI-5-138, Dezember 2005.

[15] J. Tsai, L. F. Cranor, A. Acquisti, and C. M. Fong, "What's it to you? a survey of online privacy concerns and risks," *A Survey of Online Privacy Concerns and Risks (October 2006) .NET Institute Working Paper*, no. 06-29, 2006.