PRIVATT - A Closer Look at People's Data Privacy Attitudes in Times of COVID-19

R. Trestian[1], G. Xie[2], P. Lohar[2], E. Celeste[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 current Covid-19 global pandemic led to a proliferation of contact-tracing applications meant to help control and suppress the spread of the virus. However, the success of these contact-tracing apps relies on obtaining access to sensitive data stored on citizen's mobile devices. The approaches taken are different around the world. While the countries with a strong democratic and civil liberty ethos are encouraging voluntary adoption of contact-tracing apps by their citizens, other countries opted for forced mass surveillance methods that limit individual freedoms. As a result, the attempt to fight the global pandemic is actually testing people's attitudes towards privacy and government surveillance. In this context, this research introduces a pilot study examining people's privacy concerns in a time of Covid-19. The results show that people are willing to share their personal data in the interest of controlling the spread of the virus and save lives.**

I. Introduction

Technology advances combined with the increasing affordability of mobile devices create new opportunities for responding to public health emergencies. The integration of technology in emergency response could represent a dramatic shift when dealing with public health interventions by enabling a faster coordinated response. Due to the outstanding increase in the number of users with mobile devices as well as the integration of key enabling technologies like cloud computing it is possible to create an entire tracking ecosystem that could enable the use of various surveillance methods. However, as current governance and regulation frameworks are lagging behind all these technological advancements, this triggers a highly relevant issue that is the data privacy. This is visible in the current global pandemic, where concerns around privacy and civil liberties have led the countries around the world to respond with different approaches when dealing with the spread of Covid-19 and the preservation of human life.

Apart from large-scale testing, South Korea and China were the first to adopt mass surveillance contact-tracing systems in an attempt to quickly identify the exposed population and suppress the spread of the virus. Learning from the recent experience with the Middle East Respiratory Syndrome (MERS) Coronavirus outbreak in 2015, South Korea's population accepted that a privacy trade-off is required. Thus, GPS, CCTV footage, credit card transaction, and travel information data was used by their epidemiological intelligence officers to monitor the population and ensure those infected or quarantined obey the rules, or risk being punished with a location-tracking bracelet or even incarceration [1].

China used its extensive surveillance infrastructure to contain the spread of the virus without much consideration of individual privacy rights. Health QR codes were embedded in popular mobile phone apps that generate a rating indicating the health status of an individual and their likelihood of being infected based on their travel and medical data. In the case of a person testing positive, the authorities will release public data including the person's address and movement history. Surveillance footage along with facial recognition and movement mobile phone data are used to monitor any quarantine violations which are associated with severe penalties.

These centralized mass surveillance methods enforced in South Korea and China along with mass testing have been effective in containing the spread of the virus, but have done so at the cost of population privacy rights. A different situation pertains in Europe, with the European Union General Data Protection Regulation (GDPR) affording legally enforced privacy protections regarding the collection, use, and storage of personal digital data. As contact tracing applications employ proximity data to indicate the likelihood of someone being infected based on the epidemiological distance and duration of contact with an infected person, for this approach to be successful in European countries, requires high levels of adoption and engagement from the general population, something that is difficult to achieve due to citizen information privacy concerns. For example, even in countries where data privacy is not formally at risk, citizens may have varying perceptions of what they perceive as legally permissible or safe from a fundamental rights perspective. From a socio-legal perspective, this phenomenon can be regarded as a discrepancy between formal legality and legal reality.

This research attempts to better understand the balance between the potential benefits of using a contact-tracing app, the privacy risk and legal implications as well as the enticements that influence people intention to share personal information during a pandemic. Consequently, this paper presents a survey on various contact-tracing apps adopted by different countries around the world as well as the results of a pilot study conducted in Ireland in order to investigate the attitudes to privacy of the residents of Ireland during Covid-19 times.

II. Survey of Contact-Tracing Apps

A. Contact Tracing Apps Architectures

Various Covid-19 tracing apps have adopted different architectures and different technologies for data collection in order to try to overcome the security and privacy concerns. Most of the related surveys in the literature [2]–[5] classify the contact tracing solutions into two categories, such as: centralized and decentralized as illustrated in Fig. 1.

The *centralized* architecture makes use of a centralized cloud server to store pseudonymous users' personal information, performs risk analysis and sends out notifications to close contacts in case of infection. Additionally, these data could be also used for data analysis that could help the government making informed decisions regarding the lockdown restrictions in hot-spot areas. However, there is a risk that the cloud server could become an untrustable entity which in turn triggers security and privacy concerns regarding the use and the life cycle of the data collected and stored on the server.

On the other side, the *decentralized* architecture reduces drastically the involvement of the centralized server within the contact tracing process by moving the core functions from the cloud server to the user devices. The contact tracing apps that are based on the decentralized approach do not store identifiable information at the server side as they do not require the users to pre-register prior to using the app. The devices running the contact tracing app that come in close contact will periodically exchange privacy-preserving pseudonyms. In this scenario, the cloud server acts as a rendezvous point for lookup purposes. If a user gets infected with Covid-19, they can volunteer to upload their relevant time information representing their individual trajectory. This information does not include additional data about the encounters. This type of information can be accessed regularly by other app users for local risk analysis purposes. In this way it is possible for anyone to check if they have been exposed to the virus and for how long. Consequently, the decentralized approach alleviates some of the privacy risks as compared to the centralized one. However, there is no information stored on the cloud server that could help the government making informed decisions regarding lockdown restrictions in exposed hot-spot areas.

Ahmed et al. [6] define a *hybrid* approach as a combination of the centralized and decentralized approaches. Within the hybrid architecture the centralized cloud server does not send the encounter information from the infected users to others and the risk analysis and the notifications are handled locally at the server. This approach avoids the user de-anonymisation attacks that could happen within the decentralized approach. In this case, an infected user voluntarily uploads the required data to the centralized server. Other users could check their risk exposure by inquiring the server which computes the risk analysis and notifies the users in case they need to contact the health authority. The advantage of this architecture is that statistical information is available at the server that could be used to identify exposure hot-spots and help the government decide on the required measures to be taken depending on the pandemic circumstances. However, it is not clear if this approach has been implemented in the contact tracing app. Consequently, similarly to other projects[1] in the literature, this paper uses the centralized and decentralized architectures to classify the contact tracing apps.

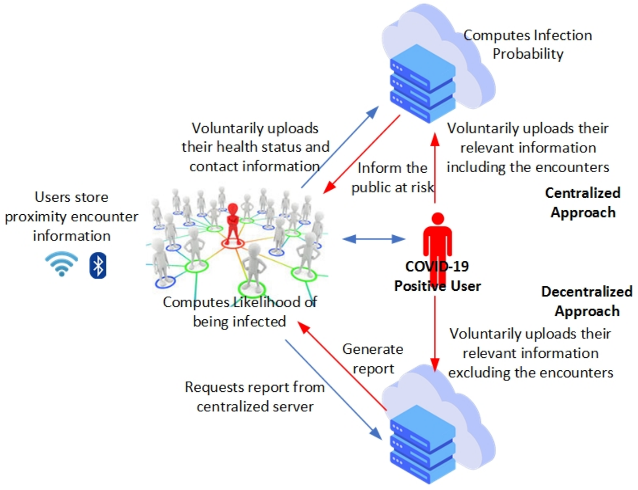
Computes Infection Probability
Voluntarily uploads their health status and contact information
Inform the public at risk
Voluntarily uploads their relevant information including the encounters
Centralized Approach
Users store proximity encounter information
COVID-19 Positive User
Decentralized Approach
Computes Likelihood of being infected
Generate report
Voluntarily uploads their relevant information excluding the encounters
Requests report from centralized server

Fig. 1: Centralized vs. Decentralized Approach of Contact Tracing Apps

B. Overview of Contact Tracing Apps

The use of centralized vs. decentralized contact tracing apps is divided around the world. The countries using the centralized apps mainly follow the PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) protocol [7] and most of these approaches predominantly rely on Bluetooth. However, some of the approaches combine the use of Bluetooth with location information to improve their accuracy. Moreover, the contact tracing apps adopted around the world provide different levels of details and even though they might have similar characteristics, the impact of the critics and the technological and privacy decisions is different from country to country.

The Corona 100m (Co100) app[2], developed in South Korea makes use of public government data to alert the users if they are within 100m of a location visited by a COVID-19 infected person. However, the users can also see the date if a COVID-19 patient was confirmed with the disease, their nationality, gender, age as well as some of their location history.

PeduliLindungi[3] was developed in Indonesia by the Ministries of Communications and Information and the State-Owned Enterprises. The app relies on the voluntary adoption by the users. Once the app is installed on their mobile devices, the users need to register as participants and share their name,

[1] Ada Lovelace Institute COVID-19 digital contact tracing tracker monitoring - https://www.adalovelaceinstitute.org/project/covid-19-digital-contact-tracing-tracker/

[2] The Corona 100m - https://bit.ly/3wuJP26

[3] PeduliLindungi - https://bit.ly/3sZwT2a

phone number, and device identifiers as well as geolocations and timestamps. Privacy concerns were raised as the app also collects additional information (WiFi MAC address and local IP address) that is not required for the app's main purpose.

Covid Symptom Tracker[4] is an app developed in UK to help the users keep track of their symptoms. Initially, the users are asked to fill in a profile where they provide personal information (e.g., age, gender, postcode, etc.) as well as existing medical conditions (e.g., heart disease, asthma, diabetes, etc.). After the profile is created, the users report their health status daily by answering questions on a wide range of symptoms. The data is shared with researchers and health officials. The authors state that the users' data is protected by the European Union's "General Data Protection Regulation" (GDPR). However, when the data is shared with the researchers in the United States it might not be protected in the same way as under GDPR.

The StopCovid[5] app developed in France to limit the spread of COVID-19 by using the Bluetooth technology for proximity tracking and identifying the transmission chains. The users would install the app on their mobile phones on a voluntary basis. However, the concerns that the technology could compromise an individuals' right to privacy could limit the voluntary adoption of the app and consequently its efficacy.

COVIDSafe App[6] developed by the Australian Government Department of Health, makes use of Bluetooth to monitor close contacts between users using the app. The app relies on voluntary adoption and requires the user to register. However, apart from the registration data, all the tracing information collected remains on the device unless the user decides to upload it in case of infection. To mitigate some of the privacy concerns the COVIDSafe app is not using the GPS and the source code of the app has been made available to the public for inspection. However, some criticism was attracted due to the amount of data held by the federal government.

Recently, most of the countries adopted the decentralized approach that relies on the cross-platform API developed by Google and Apple [8]. In the UK a centralized approach was initially adopted, but due to privacy concerns and mobile devices battery drainage, a switch was made to decentralized solution. Consequently, NHS COVID-19 App [7] is used in England and Wales for monitoring the spread of COVID-19. The app was designed using the Apple/Google Exposure Notification System to enable a decentralized operation and makes use of Bluetooth for the collection and recording of proximity encounters between communicating devices. The use of the decentralized approach is the least intrusive to privacy as most of the data is stored and processed only on the user's mobile device. The user has the option to delete the app and the data at any time.

TraceTogether[8] app was developed by the Government Technology Agency in Singapore in collaboration with the Ministry of Health (MOH). The app asks users for consent during the initial setup. Bluetooth signals will be exchanged between mobile phones running the same app when they are in close proximity (e.g., up to 5meters). The data is stored locally on the user's phone and not sent to MOH unless they are contact traced. However, if the user is asked by MOH to share the data and they do not comply, they may be prosecuted under Singapore's Infectious Diseases Act. The government made the use of the app mandatory for high risk population.

The Home Quarantine [9] app used in Poland is intended for people under quarantine. Initially, the users need to register a selfie and then periodically send geo-located selfies when prompted. The people under quarantine have a choice to either download and use the app or receive unexpected visits from the police. However, in case the users are using the app but do not comply in sending the selfie pinpointing their exact locations, the police is notified.

The Immuni [10] app developed in Italy in collaboration with the Ministries of Health and Technological Innovations and Digitalization, is based on the Apple and Google decentralized solution and uses of Bluetooth to log close contacts on the mobile device. The adoption of the app relies on the citizens' willingness to install it on their personal devices. In terms of privacy, no personal data is collected by the app and geolocation is not used. The app is in full compliance with the law-decree of April 30, 2020, n. 28 that guarantees the confidentiality, integrity, availability, and resilience of processing systems and eliminates the re-identification risk of parties whose pseudonymized data has been processed.

COVID Alert [11] developed with a privacy focus by Canadian government agencies and Shopify volunteers, makes use of Bluetooth and the Google/Apple exposure notification. The app mitigates the privacy concern by assigning a random code to every device without collecting personal information.

The Hamagen app [12] used in Israel to help prevent the spread of COVID-19, records the users' location data locally and compares the information with Health Ministry data to understand if they have crossed paths over the last 14 days, with someone who tested positively. If the app finds a match, it will notify the user to go into self-quarantine. The app works based on voluntary adoption and the users can decide if they want to report their exposure with the ministry or not.

In Ireland HSE addressed the privacy issues of their COVID Tracker[13] app by making the assessment on data protection impact of the app available to the public, and the source code of the app was also made open source. However, the Irish Council for Civil Liberties raised privacy concerns due to the lack of transparency from Apple and Google's side in terms of their involvement in the tracker app. Consequently, despite the improvements around privacy and security offered

[4] Covid Symptom Tracker - https://covid.joinzoe.com/

[5] StopCovid - https://reut.rs/3fN961H

[6] COVIDSafe https://bit.ly/31WBOVy

[7] NHS COVID-19 App https://www.covid19.nhs.uk

[8] TraceTogether https://www.tracetogether.gov.sg/

[9] Home Quarantine - https://tinyurl.com/a5d6jram

[10] Immuni - https://tinyurl.com/8t7xsjts

[11] CovidAlert - https://tinyurl.com/xvddzr78

[12] https://tinyurl.com/5998tpzk

[13] COVID Tracker Ireland https://tinyurl.com/k3h9wxxh

by the decentralized approach, there are still concerns that Google/Apple could end up controlling the EU's Covid-19 app ecosystem.

A summary of the contact tracing apps adopted by different countries around the world is given in Table I. The main concerns around the two approaches (centralized vs. decentralized) are related to the type and location of the data collected (e.g., if this is held by the government or if it remains with the users). The countries that prefer to retain control, opted for the centralized approach as in this way, the government can impose the required steps to control the spread of the virus instead of relying on the users to act on the information provided by the app. However, a comparison between the efficacy of the two approaches centralized vs. decentralized and their contribution towards slowing down the spread of Covid-19 is difficult to make due to the high number of factors involved (number of participants, population density, running duration (e.g., how long was the app running in that particular country), etc.). Despite all the efforts across the world, it is obvious that finding the balance between the potential benefits of an effective technology-based contact tracing app and the data protection and privacy of individuals remains a challenge.

III. Privacy Attitudes in Times of Covid-19

It is vital to understand the public's views on privacy considering that privacy concerns drive the technical requirements for many tracing apps. This section describes a pilot survey which was conducted to investigate the attitudes to privacy of the residents of Ireland during Covid-19 times. The study is based on anonymous questionnaire that is distributed online over the main channels and consists of three parts: (1) demographic data collection following the guidelines from [9]; (2) general privacy profiles based on the Privacy Segmentation Index (PSI) [10]; and (3) attitude towards privacy in times of Covid-19.

A total of 258 participants took part in the pilot study with the age ranging from 18 to 74 years old and a mean of 40.3. The largest age group is between 31 and 40 years old. The gender profile of respondents is 50% male, 48.8% female, 2 persons who preferred not to say and 1 person who stated they had undergone gender transformation. In terms of educational background, 35.7% of respondents hold a Master's degree, 26% hold a Doctorate degree and 22.1% a Bachelor's degree.

A. General Privacy Profiles

Three statements based on the PSI [10] were introduced to help us identify the general privacy profile of each participant. The participants were asked to rate each statement on a four-point scale from *Strongly Disagree* to *Strongly Agree*. The statements are: (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. Based on their response to these statements, the participants were classified into three groups: (a) *privacy fundamentalists* - representing individuals who are at the maximum extreme of privacy concern and the most protective of their privacy; (b) *privacy pragmatists* - representing individuals who weigh up the pros and cons of information sharing before deciding on sharing their personal information; and (c) *privacy unconcerned* - representing individuals who are least protective of their privacy. In line with Westin's classification [10] participants who agreed with statement 1 and disagreed with statements 2 and 3 were profiled as *privacy fundamentalists*. Participants who disagreed with statement 1 but agreed with statements 2 and 3 were profiled as *privacy unconcerned*, while the rest of the participants were profiled as *privacy pragmatists*.

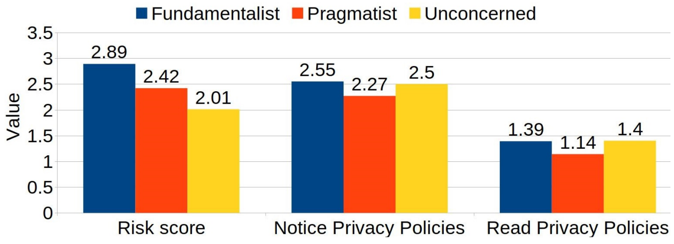

Fig. 2: Risk Attitude Responses

The results of the general privacy profiles of the participants in the pilot study indicate that the participants were: 27.5% *privacy fundamentalists*, 57% *privacy pragmatists* and 15.5% *privacy unconcerned*. These results are consistent with the results of previous Westin's surveys indicating that the majority are privacy pragmatists [10].

B. General Risk Attitude

In order to determine the level of participants' concern in relation to personal data sharing via the mobile apps that they install on their devices, the following questions were used to compute a *Risk Score* [11]:

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

The *Risk Score* was then computed by allocating points to responses and taking the average. The higher the *Risk Score* value, the greater the level of concern or perceived risk associated with using mobile apps. This method of assessing participants' concerns is reasonably reliable, as indicated through a Cronbach's α of 0.81.

Two additional questions were used to analyze the general risk attitudes of the participants. These were: (1) Do you generally notice whether or not a mobile app you want to install on your phone has a privacy policy? and (2) How often do you read mobile apps' privacy policies?

These risk attitude results are listed in Fig. 2 and grouped according to Westin's classification. Based on 2-sample t-

TABLE I: Contact-Tracing App Approaches Around the World and Technologies Involved

App Name	**Country**	**Architecture**	**Technology**	**Voluntary Adoption**	**Observations**
The Corona 100m	South Korea	Centralized	GPS location data	yes	The app collects personal location and sensitive data of the user. However, the user is notified when the data is being used.
PeduliLindungi	Indonesia	Centralized	Bluetooth, Location	yes	When within the Bluetooth radius, an anonymous ID exchange will occur which will be recorded by each device involved.
Covid Symptom Tracker	UK, USA, Sweden	Centralized	daily self-reporting	yes	Data collection includes: Personal information (e.g., age, gender, postcode, etc.), medical conditions (e.g., heart disease, asthma, diabetes, etc.), lifestyle. Collected personal data is shared with third party.
StopCovid	France	Centralized	Bluetooth	yes	The app will stop processing the data collected after six months from the end of the "health emergency state"
COVIDSafe App	Australia	Centralized	Bluetooth	yes	The information collected is used only with the user's consent. Contact data stored on a device will be automatically deleted after 21 days.
NHS COVID-19 App	UK	Decentralized (Google/Apple)	Bluetooth, QR Code	yes	Data (postcode district, QR codes, personal data) is stored and processed on the user's mobile device only.
Trace Together	Singapore	Decentralized (Google/Apple)	Bluetooth (Blue-Trace)	mandatory for high risk populations	Data collection includes mobile number and personal details including the National Registration Identity Card. However, data over 25 days old is deleted automatically.
COVID Tracker	Ireland	Decentralized (Google/Apple)	Bluetooth	yes	Data is stored on the user's mobile device only. The user can decide to share or not to share their data.
Home Quarantine	Poland	Decentralized (Google/Apple)	Bluetooth	yes	Collected data may be shared with third party
Immuni	Italy	Decentralized (Google/Apple)	Bluetooth	yes	There is no collection of personal information, neither user location. However, you need to indicate the region and province where you live.
COVID Alert	Canada	Decentralized (Google/Apple)	Bluetooth	yes	Personal data is collected by Health Canada only to support COVID-19
The Hamagen app	Israel	Decentralized	Location	yes	Collected data may be shared with third party. Location data is crossed referenced with corona patients health data.

tests, the results show that *privacy fundamentalists* had statistically significantly greater risk scores than both *privacy pragmatists* (t(216)=4.29, p<.0001) and *privacy unconcerned* (t(109)=5.95, p<.0001). The results also indicate that the *privacy fundamentalists* have a greater feeling of concern or perceived risk relating to their personal information when they are using mobile apps. However, in terms of reading and noticing the privacy policies on the mobile apps, all three groups tend to have a similar tendency.

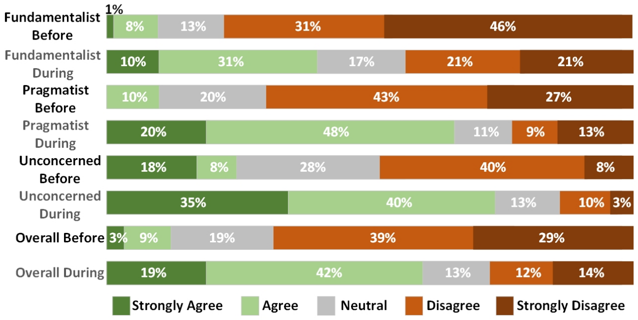

Fig. 3: Privacy Attitudes Before and During Covid-19

C. Privacy Attitudes in a Time of Covid-19

To understand if there is any shift in attitude in terms of data privacy in times of Covid-19 we compare participants' answers regarding their willingness to share their personal data (data stored on their mobile device) with the government and relevant institutions/organizations under normal circumstances vs. their willingness to do so during this specific time of pandemic to help defeat the spread of Covid-19. The results are grouped according to Westin's classification as in Fig. 3. They indicate a shift in attitude, with 61% of the participants indicating that they Strongly Agree and Agree to share their mobile data during this time of pandemic in the interest of saving lives. In terms of *privacy fundamentalists* around 31% (a combined response of Strongly Agree and Agree) of them would change their attitude towards mobile data sharing in times of Covid-19. Previous studies [11] have indicated that the more aware of privacy threats people become the higher their feeling of concern, which makes it more likely for them to be profiled as *privacy fundamentalists*, even though their actions in general might not justify their classification. The highest shift in attitude is recorded by the *privacy pragmatists* with a jump of 57%. However, regardless of their attitude shift during pandemic, 89% of the participants Strongly Agree and Agree with the statement that *Digital technologies are a necessary component to help control Covid-19 spread and monitor public health.*

IV. Formal Legality vs. Legal Reality

The participants were also asked to express their view on the use of Covid Tracker app, the mobile application introduced

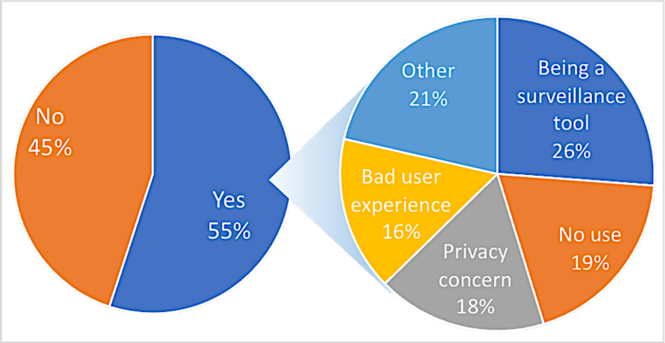

Fig. 4: Using/Not Using the HSE Covid Tracker App and related concerns of those who are using the app

in Ireland in July 2020 in order to track close contact between individuals. As shown in Fig. 4, 55% of the respondents confirmed their use of the app. However, interestingly, 26% feared that the app could be used as a surveillance tool going beyond its primary aim to fight the spread of Covid-19, another 19% of participants considered the app to be of no use and 18% stated that they had privacy concerns regarding the app.

We argue that these data show a discrepancy between formal legality and legal reality, or, in other words, between what is formally legal and what is perceived as such. Moreover, privacy concerns related to the potential misuse of mobile apps introduced to fight Covid-19 are not unfounded. For example, in some countries, contact tracing apps process location data and have been used by government for general law enforcement purposes, a circumstance that the European Data Protection Board in its Guidelines published in April 2020 has defined as *"a grave intrusion into people's privacy"* [12]. Similar risks have generated an intense debate in Europe on the safeguards that contact tracing apps should guarantee in line with EU fundamental rights. To this end, last spring, the European Commission, the European Data Protection Board and the European eHealth Network adopted detailed sets of guidance on how to deploy digital technology solutions in full respect of EU fundamental rights.

In Ireland, the Department of Health and the Health Service Executive successfully demonstrated to comply with these guidelines in developing and introducing the Covid Tracker App. Therefore, notwithstanding the formal legality of the digital solutions implemented in Ireland, the results of the pilot survey show a significant mistrust in the safeguards the Irish app is theoretically meant to guarantee. In conclusion, this image of legal reality in Ireland indicates the need to reflect on the capability of existing data protection law to be understood and instill trust at societal level.

V. Conclusions

This research presents a pilot study on the privacy attitude in times of Covid-19, of the residents of Ireland. People are mostly concerned about privacy and security issues when it comes to sharing the data and they show a lack of trust in the Government and the private players managing the data. The results indicate that although privacy and legal concerns inhibit the use of contact-tracing apps, the interest of controlling the spread of the virus and potentially preserve human life, are important factors that can outweigh privacy risk perceptions when deciding to disclose personal information during a pandemic.

VI. Acknowledgments

This work was supported by 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] D. Skoll, J. C. Miller, L. A. Saxon, "COVID-19 testing and infection surveillance: Is a combined digital contact-tracing and mass-testing solution feasible in the United States?," in *Elsevier Cardiovascular Digital Health Journal*, Oct. 2020.

[2] J. Li and X. Guo, "COVID-19 Contact-tracing Apps: a Survey on the Global Deployment and Challenges", arXiv:2005.03599 [cs], May 2020, Accessed: Oct. 21, 2020. [Online]. Available: http://arxiv.org/abs/2005.03599.

[3] V. Shubina, S. Holcer, M. Gould, and E. S. Lohan, "Survey of Decentralized Solutions with Mobile Devices for User Location Tracking, Proximity Detection, and Contact Tracing in the COVID-19 Era", Data, 2020, Accessed: Oct. 21, 2020. [Online]. Available: https://search.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/en/covidwho-784013.

[4] M. A. Azad et al., "A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications", arXiv:2006.13354 [cs], Aug. 2020, Accessed: Oct. 21, 2020. [Online]. Available: http://arxiv.org/abs/2006.13354.

[5] D. Wang and F. Liu, "Privacy Risk and Preservation For COVID-19 Contact Tracing Apps", arXiv:2006.15433 [cs], Jun. 2020, Accessed: Oct. 21, 2020. [Online]. Available: http://arxiv.org/abs/2006.15433.

[6] N. Ahmed et al., "A Survey of COVID-19 Contact Tracing Apps," *IEEE Access*, vol. 8, 2020, pp. 134577–134601.

[7] PEPP-PT Consortium, "Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)," *White Paper*, June, 2020. Accessed: Nov. 30, 2020. [Online] Available: https://github.com/pepp-pt/pepp-pt-documentation;

[8] Apple and Google, "Exposure Notification API launches to support public health agencies," *Press Release*, May, 2020. Accessed: Nov. 30, 2020. [Online]. Available: https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/;

[9] J. Hughes et al. "Rethinking and Updating Demographic Questions: Guidance to Improve Descriptions of Research Samples." *Psi Chi Journal of Psychological Research*, vol. 21, 2016, pp. 138-151.

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

[11] J. Tsai, L. F. Cranor, A. Acquisti, and C. M. Fong, "What's it to You? A Survey of Online Privacy Concerns and Risks", *Social Science Research Network*, Rochester, NY, SSRN Scholarly Paper ID 941708, Oct. 2006.

[12] European Data Protection Board, "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak," April, 2020, Accessed: Dec. 09, 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en;