



HAL
open science

Perceived Privacy Problems Within Digital Contact Tracing: A Study Among Swedish Citizens

Ali Padyab, Joakim Kävrestad

► **To cite this version:**

Ali Padyab, Joakim Kävrestad. Perceived Privacy Problems Within Digital Contact Tracing: A Study Among Swedish Citizens. 36th IFIP International Conference on ICT Systems Security and Privacy Protection (SEC), Jun 2021, Oslo, Norway. pp.270-283, 10.1007/978-3-030-78120-0_18. hal-03746054

HAL Id: hal-03746054

<https://inria.hal.science/hal-03746054v1>

Submitted on 4 Aug 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Perceived Privacy Problems within Digital Contact Tracing: A Study Among Swedish Citizens*

Ali Padyab¹[0000–0002–5286–4850] and Joakim Kävrestad¹[0000–0003–2084–9119]

University of Skövde, Sweden *firstname.lastname@his.se*

Abstract. Several governments employed digital contact tracing using smartphone apps to combat the COVID-19 pandemic in 2020. Research shows that privacy concerns hinders adoption of such apps, while privacy problems which emerged by using them are empirically unknown. The aim of this study is to uncover the dimensions of privacy problems available in digital contact tracing through a survey from 453 citizens in Sweden. Our results show that respondents found privacy problems regarding surveillance, identification, aggregation, secondary use, disclosure, and stigma highly relevant in contact tracing apps. Among demographic factors, younger respondents were generally more concerned about privacy risks than older respondents. This study extends previous literature by revealing privacy problems arising from contact tracing apps.

Keywords: Digital contact tracing · Privacy · Surveillance · Identification · Aggregation · Secondary use · Disclosure · Stigma.

1 Introduction

Digital contact tracing has been utilized by many governments throughout the globe as a strategy to slow down the quick spread of COVID-19. Several novel software applications (Apps) have been developed in many countries to combat the pandemic. The purpose of contact tracing apps is to use information and communication technologies to automate the process of identifying and notifying contacts of an infected person, and to map the route of disease transmission spread.

Compared to its manual process, digital contact tracing demands less labor and hastens to keep up with the current COVID-19 outbreak [7] [11]. Many studies have explored contact tracing apps in the light of their adoption [32], design [3], technical features [29], effectiveness [6], legal [13], facilitators and barriers [19]. However, digitization of the process has raised an important concern about individual's privacy [7]. In a national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland, citizens raised concerns regarding privacy and data security [21]. Similar results surfaced in surveys conducted in

* Supported by VINNOVA

the Netherlands, France, Germany, Italy, the United Kingdom, and the United States where citizens mentioned privacy as a strong reason not to use the contact tracing mobile applications [15][5]. Therefore, understanding the nuances of an individual’s privacy concerns toward contact tracing apps is a central consideration needed to maintain public trust [7].

To this end, research on privacy aspects of contact tracing apps is limited to the perspectives of researchers and their opinions, whilst empirical studies emanating from citizens’ privacy concerns are absent in digital contact tracing. Hence, more research is needed to uncover the dimensions of privacy risks available in digital contact tracing [21][6]. Therefore, the current study aims to address the following research questions: 1) How citizens perceive potential privacy problems related to digital contact tracing? and 2) How do various demographic factors affect perceived privacy problems by the citizens? To investigate the relationship between contact tracing apps and privacy concerns, we conducted a survey with 453 respondents in Sweden. The results showed that there is a meaningful relationship between perceived privacy problems and use of contact tracing apps. Moreover, the results will have implications to the development of effective privacy-protective mechanisms and policies that stem from citizen’s privacy concerns.

The rest of this article is structured as follows: we first review the privacy problems emerged from the digital contact tracing within the COVID-19 pandemic era in section 2 followed by the methodology employed in section 3. In section 4, we present the results and finally, we conclude the paper with indicating future direction of research in section 5.

2 Background

Privacy according to Goodwin (1991) [12] is considered as an elastic and vague concept with a wide variety of definitions. Within these varied definitions of privacy, Solove (2006) [26] has attempted to focus on privacy harms or problems rather than creating a shared meaning. His taxonomy of privacy embodies sixteen different privacy violations for contemporary times [26]. For the purpose of the present study, privacy violations most relevant to contact tracing were considered for various reasons, among others, so that our study wouldn’t be too extensive to report about in a conference paper. Yet, future research which includes more elements from Solove’s taxonomy would be of great importance and interest. Below, we discuss the potential privacy violations from the taxonomy that we deemed most problematic in a typical contact tracing app:

2.1 Surveillance

Surveillance refers to “watching, listening to, or recording of an individual’s activities” [26]. In digital contact tracing, surveillance is related to keeping track of app users, the contacts of an infected person, and their activities. Even if the person is not infected, the contacts and encounters are recorded, giving rise

to more detailed surveillance on a person’s movement, identity, mental health, social behavior, and associations (e.g., [23]).

2.2 Identification

According to Solove (2006) [26], “Identification is linking information to particular individuals”. Depending on its implementation, contact tracing apps collect various information related to users (and contacts) such as personal information, device identifiers, and locations coordinates. Aggregation and performing data analytics on data extracted from various databases (e.g. health authorities and smart cities) makes it possible to make the identity of the users and their contacts known [9]. Research shows that both centralized and de-centralized systems suffer from the risk that people could be deanonymized [31].

2.3 Aggregation

“Aggregation involves the combination of various pieces of data about a person” [26]. Observation from countries such as China and South Korea shows that digital contact tracing apps were not sufficient to trace contacts, but more technologies were combined to even invade to private zones of individuals. Data from CCTVs and GSM/Cell towers/WiFi location were collected to be used through face recognition to co-traveler techniques to create more detailed movement patterns of individuals [22]. Early research indicates the accumulation of other potential types data such as data from social media platforms, credit card transactions, travel booking data, and other surveillance data points [24].

2.4 Secondary use

Secondary use refers to “the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject’s consent” [26]. In the context of contact tracing apps, secondary use could cause harm if a data holder shares and/or conducts additional processes to extract information about users, the pandemic (or not related to the pandemic) beyond their awareness. Here, the role of AI and Big data analytics is highlighted for various purposes such as de-identification of location histories, movement patterns, psychological behavior, and many more. Needless to say, it is possible to infer information about the user’s whereabouts and track their location via fixed-location sensors, rouge devices, or QR-codes (e.g. NZ COVID Tracer app [33]).

2.5 Disclosure

“Disclosure involves the revelation of truthful information about a person that impacts the way others judge her character” [26]. Disclosure occurs in different ways within digital contact tracing. Spread of information about an infected person and his or her location to other contacts and government bodies is a

reported privacy issue during the COVID-19 pandemic [34]. Another privacy violation occurs when an individual's contacts are disclosed, which may be considered private or controversial. For example, during the COVID-19 outbreak in a LGBTQ district in Seoul concerns were voiced in the gay community in the case of those who had not disclosed their sexuality to employers or family [10].

2.6 Stigma

In Solove's taxonomy, distortion "involves the spreading of information that affects the way society views a person ... distortion differs from disclosure, however, because with distortion, the information revealed is false and misleading" [26]. Stigma is a type of privacy harm emanated because of distortion. Studies from contact tracing for tuberculosis shows that a consequence of the identification of close contacts of infected cases is social stigma [2]. In contact tracing of COVID-19 infection many cases have been reported to "out" patients, false identifications, witch-hunts and abuse towards those who spread the virus with nicknames such as "super propagator", "super contaminator" or "super spreader" [27][10][17].

2.7 Perceived privacy problems and digital contact tracing apps

In the context of mobile apps, privacy violation is undesirable. Bansal et al (2010) found in their study of E-Health records that individual's concern for information privacy has direct influence on attitude to "opt-in" and share personal health information [1]. Contact tracing apps are not exempted from mobile apps and various studies have pointed towards the privacy concerns of citizens in using such apps despite their perceived benefits [15][21][5]. It is reasonable to assume from the above arguments that those who are positive towards using an application for contact tracing will be less concerned with privacy issues relating to the application.

3 Methodology

This paper seeks to evaluate how Swedes perceive potential privacy issues related to contact tracing applications, and how various demographic factors affect this perception. A web-based survey was deemed a suitable approach for exploring this notion and we aimed to gather responses from at least 400 respondents. The survey began with a description of contact tracing apps which was followed by two question sections. The first section contained demographic questions and the second section contained one Likert scale with five statements for each of the six included dimensions of privacy concern. Likert scales were used because of their frequent prior use in research when measuring perceptions and opinions of a population [16]. All questions were followed by a free-text field where the respondents could elaborate on their responses. The statements and questions in the survey will be outlined in the result section. Prior to distribution, the

survey was subjected to pilot testing during which it was distributed to a small population and 35 answers were collected. Two peers, one with a background in information security and one with a background in statistics, were asked to review the survey in depth.

To generate a probability sample, a stratified sampling approach was used [14]. The population, Swedes, was divided into subgroups based on gender, age, and geographical region. Equal proportions of each subgroup were recruited to the survey using simple random sampling [25]. The practical sampling was performed by the survey provider Webropol, using their web panel. As such, the range of possible participants was restricted to members of their panel. Using a web panel has been suggested to provide a higher level of data reliability than surveys administered over telephones since it reduces the researcher bias [8].

The survey data was analyzed using the software SPSS¹. As described by Joshi et al. (2015) [16], Likert scales assume that all statements in the scale measure the same underlying concept. Thus, Cronbach's Alpha was used to measure the internal consistency of each scale [28]. Cronbach's Alpha returns a value between 0 and 1 and a value over 0.65 is typically considered appropriate for studies with human participants, and was adopted as the threshold of acceptance for this study [30]. Next, the answers in each scale were transformed to an index value reflecting the composite score for each scale, allowing for parametric analysis [16]. Finally, answer groups were constructed based on the demographic questions and independent sample T-tests used to identify statistically significant differences between groups. The conventional significance level of 95% was used and T-test is considered to be robust regardless of distribution form given the relatively large sample in this study [20]. However, Mann-Whitney U-test was also used as a means of triangulation to increase the validity of the results [18]. When a statistically significant difference was identified, Pearson's correlation coefficient was computed to further analyze how the demographic affected the privacy concern. Pearson's correlation coefficient is a value between -1 and 1 and describes the linear correlation between two variables. -1 or 1 show perfect correlations while correlations under 0.3 or -0.3 are considered weak [4].

4 Results

After pilot testing, the survey was sent out to 2020 possible respondents and it was open for one week. 453 respondents answered the survey leading to an answer rate of 22%. The respondents were first asked five demographic questions. The questions (translated from Swedish) and proportions of respondents for each option is reflected in Table 1.

Following the demographic questions, the participants were provided with the following text (translated from Swedish) describing the concept of contact tracing applications:

This survey is about how you perceive integrity in relation to contact tracing applications. This type of apps can effectively support infection

¹ <https://www.ibm.com/analytics/spss-statistics-software>

Question	Answer	Proportion
As what gender do you identify?	Male	51.7%
	Female	41.8%
	Other/Prefer not to say	0.2%
What is your highest level of education?	Elementary school	3.1%
	High-school	33.1%
	Higher education, 3 years or less	24.1%
	Higher education, more than 3 years	38%
	Doctoral education	1.8%
How old are you?	18-27	12.6%
	28-37	20.5%
	38-47	19.2%
	48-57	19.6%
	58-67	20.5%
	Above 67	11.3%
What is your main occupation?	Student	10.2%
	Working full time	54.3%
	Working part time	6.4%
	Retired	18.3%
	Business owner	4.6%
	Unemployed	3.5%
	Other/Prefer not to say	2.6%
What is the best description of where you live?	City, more than 250 000 inhabitants	29.4%
	City, more than 100 000 inhabitants	15.9%
	Town, more than 50 000 inhabitants	13.7%
	Town, more than 10 000 inhabitants	17.4%
	Community, more than 5000 inhabitants	7.7%
	Community, more than 1000 inhabitants	4.4%
	Smaller community/countryside	11.5%

Table 1. Demographic properties of the sample

tracing and could have been used during the corona pandemic. The purpose of such an application is to keep track of persons that come in contact with each other in a way that could result in a spread of infection. To do this, the application needs to know where you are and sense who you are in contact with. It will also need to know if you are infected or not.

For this survey, we want you to imagine such an app and rate how well you agree with a number of statements. 1 means that you do not agree at all, and 5 means that you fully agree. Assume that the information in the application is shared between you and the healthcare system, unless stated otherwise.

Six themes will be described to you and we want you to respond to five statements for each theme.

The first of the six analyzed themes was *Surveillance* and the statements in this theme intended to evaluate respondents' concerns with privacy issues relating to it. The respondents were asked to rate how well they agreed with the statements on a 5-pointed scale (1= Do not agree at all and 5 = Fully agree). One statement was reversed, meaning that fully agree signified a low level of concern. The answers to the reversed statements were flipped, and Cronbach's Alpha was used to measure the internal consistency of the scale, resulting in an alpha value of 0.807. Then, the mean answers to all statements were summarized and divided by 5 to compute an index value for the theme. Note that the analysis process was identical for all six themes but will not be described in detail for themes two to six to conserve space.

Table 2 displays, the statements and data generated during the analysis.

Statement	Mean	Index	95% CI
Surveillance is never good	3.17	3.18	3.09-3.26
This kind of monitoring is worth it, considering the benefits	3.19		
I worry that my data will be used to monitor what I do. For instance my mental health and social behavior	3.34		
I believe that the collected data will be used by governments for other purposes than infection tracing	3.13		
I believe that my activity will be tracked even if I am not infected	3.45		

Table 2. Results in the theme Surveillance

The second theme was *Identification* and the Alpha for the scale was 0.754. Table 3 displays the results of the theme. Note that statements one and two were reversed in the creation of the index.

Statement	Mean	Index	95% CI
It is good if such an application can help me identify infected persons I've have been in contact with	3.24	3.33	3.25-3.41
It is good if such an application can notify persons I've been in contact with while I've been infected	3.30		
Such an application should never spread my identity, even if it means that I cannot be identified to others as infected	3.67		
Such an application should only tell where an infected person has been, not the person's identity	3.63		
I think the collected data should be anonymous	3.90		

Table 3. Results in the theme Identification

The third theme was *Aggregation* and the Alpha for the scale was 0.752. Table 4 displays the results of the theme. Note that statements one, four and five were reversed in the creation of the index.

Statement	Mean	Index	95% CI
It is okay for governmental bodies to combine information about me if it limits the spread of infection	3.19	3.33	3.25-3.41
I care about how governmental bodies share information about me	4.03		
I worry that data from a contact tracing app could be aggregated with data from other sources (e.g. social media)	3.47		
I want data from such an application to be combined with data from other sources to provide me with general health information	2.22		
It is okay if data from different sources are combined for research	3.45		

Table 4. Results in the theme Aggregation

The fourth theme was *Secondary use* and the Alpha for the scale was 0.848. Table 5 displays the results of the theme.

The fifth theme was *Disclosure* and the Alpha for the scale was 0.788. Table 6 displays the results for the fifth theme. Note that statement five was reversed in the creation of the index.

The sixth theme was *Stigma* and the Alpha for the scale was 0.762. Table 7 displays the results for the theme. Note that statements two and five were reversed in the creation of the index.

The final question asked the respondents to answer "yes" or "no" to whether they would use a contact tracing application. 34.44% (156) respondents answered "yes" and 65.56% (297) answered "no".

Statement	Mean	Index	95% CI
I worry that the collected information will be used by others outside the healthcare system	3.92	3.97	3.88-4.05
I worry that AI can be used to extract information not related to a pandemic	3.84		
I worry that , for instance, banks and insurance companies can use the information to decide my fee or interest rates	3.51		
I worry that data about my contacts can be sold or handed to companies	3.97		
Information in such an application should only be used for its intended purpose	4.59		

Table 5. Results in the theme Secondary use

Statement	Mean	Index	95% CI
I worry that if I get infected, that information will be spread to other than my contacts	3.08	3.57	3.48-3.65
I worry that information about my location can be freely available for anyone	3.86		
I worry that information about my contacts will be available to healthcare providers	3.05		
I worry that information about my contacts will become available to others than healthcare providers	3.89		
Information collected by the application should be made freely available to government bodies	2.03		

Table 6. Results in the theme Disclosure

Statement	Mean	Index	95% CI
I would worry about being branded as "Corona-infected" if I used such an application	2.32	2.73	2.65-2.82
I want others to know if one of my family members is infected by corona	2.50		
I would worry that my friends would dissociate themselves from me if they found out from such an application that I was infected	2.10		
I would worry that my employer and my colleagues would discriminate me if they found out that I was infected from such an application	2.53		
An application that can tell who is infected would make my social life easier	2.79		

Table 7. Results in the theme Stigma

Following the univariate analysis, sub-groups were created within the sample to identify demographic differences relating to privacy concerns in the six themes. Independent sample T-test was used as the primary means of hypothesis testing and Mann-Whitney U-test was used for validation purposes. The hypothesis tested for each demographic was expressed as follows:

Demographic X will affect how privacy problems in theme Y is perceived by the respondents

The corresponding null hypothesis was that no such difference could be observed. The remainder of this chapter will account for the groups created and hypotheses tested, statistics will only be provided in cases where the hypothesis is supported, for the purpose of saving space.

The first demographic was gender and the sample was divided based on the genders Male and Female, the option "Other/Prefer not to say" option was only selected by a single respondent and was subsequently disregarded in this analysis. Statistically significant differences between the gender groups could not be identified for any theme, and the null hypothesis is accepted for the demographic gender.

Next, level of education was analyzed. Two group sets were created for this purpose. First, we tested for differences between respondents with or without a degree from higher education and then we tested for differences between respondents with a doctoral degree or more than three years of higher education and the rest. No statistically significant differences could be identified, and the null hypothesis is accepted for the demographic education level.

Next, the impact of age was analyzed. Respondents aged 48 or more (n=216) were placed in one group and the rest (n=237) in the other group. Statistically significant differences were identified for four of the themes as seen in Table 8.

Theme	Group	Mean	T-test(p)	Mann-Whitney(p)	Corr coef.
Surveillance	≤ 47	3.30	0.002	0.001	-0.161
	≥ 48	3.03			
Identification	≤ 47	3.50	0.000	0.000	-0.233
	≥ 48	3.15			
Aggregation	≤ 47	3.41	0.032	0.033	-0.110
	≥ 48	3.24			
Stigma	≤ 47	2.82	0.047	0.026	-0.105
	≥ 48	2.64			

Table 8. Analysis of how age affects privacy concerns (Results are significant when $p < 0.05$). All reported correlations are significant at the 95% level.

As seen in Table 8, the results of the analysis suggest that younger respondents are more concerned about privacy aspects than older respondents. However, the correlation coefficients suggest that the relationship between the variables is weak. As such, the analysis concludes that age does affect how concerned

a person is with privacy aspects relating to Surveillance, Identification, Aggregation and Stigma. However, the correlation coefficient suggests that the power of the relationship is low.

The next demographic to be analyzed was main occupation. To generate evenly sized groups, respondents who reported working full time were placed in one group and all others in the other group. No significant differences could be identified and the null hypothesis is accepted for the demographic occupation.

Next, the impact of place of living was analyzed and grouping variables created in three ways:

- Group 1: Respondents living in cities with more than 250 000 inhabitants, group 2: the rest
- Group 1: Respondents living in cities with more than 100 000 inhabitants, group 2: the rest
- Group 1: Respondents living in towns with more than 50 000 inhabitants, group 2: the rest

No significant differences could be observed and the null hypothesis is accepted for the demographic "place of living".

The final aspect to be analyzed was if the respondents' answers differed based on their willingness to use an application for contact tracing. The hypothesis in this case being that *Respondents who are positive towards using an application for contact tracing will be less concerned with privacy issues relating to the application*. The results of this analysis is presented in Table 9. Note that no correlation coefficient was computed since the willingness to use variable is dichotomous.

Theme	Group	Mean	T-test(p)	Mann-Whitney(p)
Surveillance	Yes	2.68	0.000	0.000
	No	3.44		
Identification	Yes	2.90	0.000	0.000
	No	3.56		
Aggregation	Yes	2.87	0.000	0.000
	No	3.57		
Secondary use	Yes	3.61	0.000	0.000
	No	4.15		
Disclosure	Yes	3.13	0.000	0.000
	No	3.80		
Stigma	Yes	2.23	0.000	0.000
	No	3.00		

Table 9. Analysis of whether respondents who are positive towards using an application for contact tracing will be less concerned with privacy issues relating to the application (Results are significant when $p < 0.05$).

5 Discussion and Conclusion

The aim of this study was to research: 1) How citizens perceive potential privacy problems related to digital contact tracing? and 2) How various demographic factors affect perceived privacy problems by the citizens?

A survey-based method was used to answer those questions and a stratified sampling approach was used to acquire a probability sample representative for the Swedish population. Indexes were created based on the survey data and reflected the respondents' level of concern about privacy risks related to six aspects of privacy derived from [26]: Surveillance, Identification, Aggregation, Secondary use, Disclosure, and Stigma.

In response to the first research question, the results reflect that the respondents are somewhat concerned about privacy risks in all themes. However, while the results for most themes are just above 3, which signifies a neutral standpoint, it is notable that the concerns for secondary use of data is close to 4, suggesting that the respondents are highly concerned about their data being used for other purposes than contact tracing. This is emphasized by looking at the mean values for individual statements, where statements relating to unpurposeful use of the data is generating a higher level of concern than other statements. The second notable conclusion in relation to the first RQ is that the respondents are generally less concerned about stigma coming from the use of the application.

In response to the second RQ, the impact of several demographic factors was evaluated but the only demographic factor that had any impact on the results was age. Younger respondents were generally more concerned about privacy risks than older respondents. However, even this effect was small suggesting that the results are general across Swedish population. A previous study showed that age is an important predictor of the acceptance of COVID-19 mobile applications [15]. Our results suggest that privacy could play a mediating role between age and contact tracing app use and therefore interesting for future research to investigate. The respondents were asked to state if they would install and use an application for contact tracing and 34% responded that they would. It should be noted that this question was asked last and the result should be interpreted in the light of the possibility that the survey itself affects the respondents, positively or negatively. Using the responses to this question as a grouping variable revealed that respondents willing to install the application were significantly less concerned with privacy issues compared to those not willing to install the application. This was true for all the included themes, suggesting that privacy concern is an important factor when it comes to deciding to use an application or not. This further suggests that minimizing privacy issues and concerns is an important factor in successful deployment of a contact tracing application that needs to be used by the general public. That recommendation is a practical contribution of this study.

This study contributes with insight about how Swedish users perceive privacy risks with contact tracing applications. The results of the current study is in agreement with previous research indicating that privacy protection is critical if the contact tracing app is to be adopted [21][5][15]. This study extends previous

literature in revealing privacy problems that arise from contact tracing apps, making this one the first in its domain. Nevertheless, a limitation of the study is that it was conducted with Swedish individuals only and the degree to which the results can be generalized outside of this population is unknown and should be further studied in future research, especially given that privacy concerns are known to be perceived differently in different nations. A second limitation is that this study is focused on six of the privacy dimensions presented by [26]. Future work could be expanded to cover more dimensions.

References

1. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems* **49**(2), 138–150 (2010)
2. Critical changes to services for tb patients during the covid-19 pandemic. *The International Journal of Tuberculosis and Lung Disease* **24**(5), 542–544 (2020)
3. Abeler, J., Bäcker, M., Buermeyer, U., Zillessen, H.: Covid-19 contact tracing and data protection can go together. *JMIR mHealth and uHealth* **8**(4), e19359 (2020)
4. Akoglu, H.: User’s guide to correlation coefficients. *Turkish journal of emergency medicine* **18**(3), 91–93 (2018)
5. Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., Abeler, J.: Acceptability of app-based contact tracing for covid-19: Cross-country survey study. *JMIR Mhealth Uhealth* **8**(8), e19857 (Aug 2020)
6. Anglemyer, A., Moore, T.H., Parker, L., Chambers, T., Grady, A., Chiu, K., Parry, M., Wilczynska, M., Fleming, E., Bero, L.: Digital contact tracing technologies in epidemics: a rapid review. *Cochrane Database of Systematic Reviews* (8) (2020)
7. Bengio, Y., Janda, R., Yu, Y.W., Ippolito, D., Jarvie, M., Pilat, D., Struck, B., Krastev, S., Sharma, A.: The need for privacy with public digital contact tracing during the covid-19 pandemic. *The Lancet Digital Health* (2020)
8. Braunsberger, K., Wybenga, H., Gates, R.: A comparison of reliability between telephone and web-based surveys. *Journal of Business Research* **60**(7), 758–764 (2007)
9. Cyphers, B., Gebhart, G.: Apple and google’s covid-19 exposure notification api: Questions and answers
10. Döring, N.: How is the covid-19 pandemic affecting our sexualities? an overview of the current media narratives and research hypotheses. *Archives of Sexual Behavior* **49**(8), 2765–2778 (2020)
11. Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., Fraser, C.: Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing. *Science* **368**(6491) (2020)
12. Goodwin, C.: Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing* **10**(1), 149–166 (1991)
13. Guinchard, A.: Our digital footprint under covid-19: should we fear the uk digital contact tracing app? *International Review of Law, Computers & Technology* pp. 1–14 (2020)
14. Henry, G.T.: *Practical sampling*, vol. 21. Sage (1990)

15. Jansen-Kosterink, S.M., Hurmuz, M., den Ouden, M., van Velsen, L.: Predictors to use mobile apps for monitoring covid-19 symptoms and contact tracing: A survey among dutch citizens. (2020)
16. Joshi, A., Kale, S., Chandel, S., Pal, D.K.: Likert scale: Explored and explained. *Current Journal of Applied Science and Technology* pp. 396–403 (2015)
17. Lanese, N.: 'superspreader' in south korea infects nearly 40 people with coronavirus, <https://www.livescience.com/coronavirus-superspreader-south-korea-church.html>
18. Lincoln, Y.S., Guba, E.G.: *Naturalistic inquiry*, vol. 75. Sage (1985)
19. Megnin-Viggars, O., Carter, P., Melendez-Torres, G., Weston, D., Rubin, G.J.: Facilitators and barriers to engagement with contact tracing during infectious disease outbreaks: A rapid review of the evidence. *PloS one* **15**(10), e0241473 (2020)
20. Norman, G.: Likert scales, levels of measurement and the “laws” of statistics. *Advances in health sciences education* **15**(5), 625–632 (2010)
21. O’Callaghan, M.E., Buckley, J., Fitzgerald, B., Johnson, K., Laffey, J., McNicholas, B., Nuseibeh, B., O’Keeffe, D., O’Keeffe, I., Razzaq, A., et al.: A national survey of attitudes to covid-19 digital contact tracing in the republic of ireland. *Irish Journal of Medical Science (1971-)* pp. 1–25 (2020)
22. Park, O., Park, Y.J., Park, S.Y., Kim, Y.M., Kim, J., Lee, J., Park, E., Kim, D., Jeon, B.H., Ryu, B., et al.: Contact transmission of covid-19 in south korea: Novel investigation techniques for tracing contacts. *Osong Public Health and Research Perspectives* (1) (2020)
23. Park, S., Choi, G.J., Ko, H.: Information technology–based tracing strategy in response to covid-19 in south korea—privacy controversies. *Jama* (2020)
24. Riemer, K., Ciriello, R., Peter, S., Schlagwein, D.: Digital contact-tracing adoption in the covid-19 pandemic: It governance for collective action at the societal level. *European Journal of Information Systems* pp. 1–15 (2020)
25. Scheaffer, R.L., Mendenhall III, W., Ott, R.L., Gerow, K.G.: *Elementary survey sampling*. Cengage Learning (2011)
26. Solove, D.J.: A taxonomy of privacy. *U. Pa. L. Rev.* **154**, 477 (2005)
27. Sotgiu, G., Dobler, C.C.: Social stigma in the time of coronavirus disease 2019 **56**(2) (2020)
28. Tavakol, M., Dennick, R.: Making sense of cronbach’s alpha. *International journal of medical education* **2**, 53 (2011)
29. Trivedi, A., Vasisht, D.: Digital contact tracing: Technologies, shortcomings, and the path forward. *SIGCOMM Comput. Commun. Rev.* **50**(4), 75–81 (Oct 2020)
30. Vaske, J.J., Beaman, J., Sponarski, C.C.: Rethinking internal consistency in cronbach’s alpha. *Leisure Sciences* **39**(2), 163–173 (2017)
31. Vaudenay, S.: Centralized or decentralized? the contact tracing dilemma. *Cryptology ePrint Archive*, Report 2020/531 (2020), <https://eprint.iacr.org/2020/531>
32. Walrave, M., Waeterloos, C., Ponnet, K.: Adoption of a contact tracing app for containing covid-19: A health belief model approach. *JMIR public health and surveillance* **6**(3), e20572 (2020)
33. Yang, F., Heemsbergen, L., Fordyce, R.: Comparative analysis of china’s health code, australia’s covidsafe and new zealand’s covid tracer surveillance apps: a new corona of public health governmentality? *Media International Australia* pp. 1–16 (2020)
34. Zastrow, M.: South korea is reporting intimate details of covid-19 cases: has it helped? *Nature* (2020)