SARS-CoV-2, a Threat to Privacy?

submitted as a part of WirVsVirus Hackathon 21-21/03/2020

T. Daubenschütz, O. Kulyk, S. Neumann, I. Hinterleitner, F. Scheible, C. Hoffmann and P. Ramos Delgado

***Abstract*—The global SARS-CoV-2 pandemic is currently putting heavy strain on the world's critical infrastructures. With healthcare systems and internet service providers already struggling to provide reliable service, some operators may, intentionally or unintentionally, lever out privacy-protecting measures to increase their system's efficiency in fighting the virus. And though it may seem all encouraging to see the effectiveness of authoritarian states in battling the crisis, we the authors of this paper, would like to raise the community's awareness towards developing more effective means in battling the crisis without the need to limit fundamental human rights.**

***Keywords*—COVID-19, SARS-CoV-2, pandemic, privacy, security, critical infrastructure**

I. Introduction

DUE to its fast spreading throughout the world, the outbreak of SARS-CoV-2 has become a global crisis putting stress on the current infrastructure, in some areas in unprecedented ways making shortcomings visible. Since there is no vaccination against SARS-CoV-2, the only way to deal with the current situation are nonpharmaceutical interventions (NPI's), to reducing the number of new infections and flatten the curve of total patients.

Having a look to European states as Italy, Spain, France or Austria which are in lockdown, keeping people away from seeing each other, their right of living a self-determined life is not given anymore. As shown by Hatchett et al. this method showed a positive effect in St. Luis during 1918's influenza pandemic [1], yet, its long-term effects on economy and day-to-day life, including psychological effects on people forced to self-isolate, are often seen as a cause of concern [2]. Furthermore, some models show a possibility of a massive rise of new infections after the lockdown is ended [3].

Hence, alternative ways of handling the situation are discussed and applied, among them, mass surveillance. An example of this approach can be seen in Asian countries e.g. South Korea [4] and Singapore [5] where, besides of extensive testing, methods such as tracing mobile phone location data in order to identify possible contact to infected persons [6].

Tim Daubenschütz, dist=rtion.com, https://timdaub.github.io/, tim@daubenschuetz.de

Oksana Kulyk, IT University of Copenhagen, https://okskulyk.github.io, okku@itu.dk

Stephan Neumann, stephanneumann@tutamail.com

Isabella Hinterleitner, hinterleitner@techmeetslegal.at https://techmeetslegal.at/ueber-mich

Florian Scheible, Umit-Privat University for Health Sciences, Medical Informatics and technology, florian.scheible@protonmail.com

Carmen Hoffmann, Universität Innsbruck, carmen.hoffmann@protonmail.com

Paula Ramos Delgado, ramosdelgado.paula@gmail.com

Similar measures are taken in other countries. For instance, Netanyahu, Israel's Prime Minister ordered Shin Bet, a domestic spy agency, to start cellphone surveillance on citizens. Persons which have been closer than two meters to an infected person are receiving text messages telling them to go into immediate home isolation for 14 days. As Shin Bet mandate is to observe and fight middle easter terrorism, naturally, Israel's citizens are now concerned this is suddenly used to help aid a medical situation [7], [8], [9]. Within the EU, in particular in Germany and Austria, telecommunications providers are already providing health organisations and the government with anonymous data of mobile phone location data [10].

These measures, while being critical in managing the pandemic, raise concerns from privacy experts as the massive collection of data can easily lead to harming the population and violating their human rights if the collected data is misused. In this paper we discuss the privacy issues that can arise in times of crisis and take a closer look into the case of the German Robert Koch Institute receiving data from Telekom. We conclude with providing some recommendations about ways to minimize privacy harms while combating the pandemic.

II. Privacy

In this section we outline the general definitions of privacy, including describing the contextual integrity framework for reasoning about privacy, and discuss privacy harms that can occur from misuse of personal data. We furthermore discuss the issues with privacy that can occur during a crisis such as this global pandemic and what can be done to ensure information security and hence appropriate data protection.

A. Definitions of Privacy

Privacy is a broad concept which has been studied from the point of view of different disciplines, including social sciences and humanities, legal studies and computer science. The definitions of privacy are commonly centered around seeing privacy as *confidentiality* (preventing disclosure of information), *control* (providing people with means to control how their personal data is collected and used) and *transparency* (ensuring that users are aware of how their data is collected and used, as well as ensuring that the data collection and processing occurs in a lawful manner) [11].

Hannah Arendt, a Jewish philosopher who grew up in Germany in the beginning of the 20th century defined privacy within the context of public and private space. Her claim was that if there exists public space, there is also private

space. Arendt considers the privacy concept as "distinction between things that should be shown and things that should be hidden" [12]. And that, private spaces exist in opposition to public spaces. Meaning, while the public square is dedicated to appearances, the private space is devoted to the opposite — to hiding and privacy. She associated privacy with the home. Due to the fact that we have become used to a "digital private space", such as our own email inbox or personal data on the phone, people are concerned and offended when the private, hidden space is violated. However, in times of crisis the term hidden or privacy becomes a new meaning.

Helen Nissenbaum, a Professor of Information Science, proposed the concept of *contextual integrity* as a framework to reason about privacy. According to her framework, privacy is defined as *adhering to the norms of information flow* [13]. These norms are highly contextual: for example, it is appropriate for doctors to have access to the medical data of their patients, but in most cases it is inappropriate for employers to have access to medical data of their workers. Nissenbaum distinguishes between the following five principles of information flow [14]: the *sender*, the *subject*, the *receiver*, the *information type* and the *transmission principle* (e.g. whether confidentiality has to be preserved, whether the data exchange is reciprocal or whether consent is necessary and/or sufficient for the appropriateness of the data exchange). The norms governing these parameters are furthermore evaluated against a specific context, including whether the information flow is necessary for achieving the purpose of the context.

B. Privacy Harms

Data misuse can lead to different kinds of harms that jeopardise physical and psychological well-being of people as well as the overall society (see e.g. Solove, 2008). One of them is persecution by the government – this might not be a big concern in democratic societies, but democratic societies can move into more authoritarian governance styles, especially is crisis situations. Even if this does not happen, there are other harms, e.g. a so called "chilling effect", where people are afraid to speak up against the accepted norms when they feel that they are being watched. Furthermore, harms can result from data leaks, like unintentional errors or cyberattacks. In these cases, information about individuals may become known to unintended targets. This can result in physical harm, stalking and damage of the data subject's personal relationships. Knowledge about one's medical data can lead to job discrimination. Leaked details about one's lifestyle can lead to raised insurance rates. Leakage of location data, in particular, can reveal a lot of sensitive information about an individual, such as the places they visit, which might in turn result in dramatic effects when revealed. Just think of closeted homosexuals visiting a gay clubs or marginalized religious minorities visiting their place of worship. Even beyond these concerns, access to large amounts of personal data can be used for more effective opinion and behavior manipulation, as evidenced by the Cambridge Analytica scandal [15].

In summary, absence of privacy has a dramatic effect on our freedom of expression as individuals and on the well-functioning of the society as a whole. It is therefore important to ensure that the damage to privacy is minimized even in times of crisis.

C. Privacy in Times of Crisis

When we are considering the example of doctors treating their patients, we can use the framework of contextual integrity to reason about the appropriate information flow as follows: the patient is both the sender and the subject of the data exchange, the doctor is the receiver, the information type is the patient's medical information, the transmission principle includes, most importantly, doctor-patient confidentiality aside from public health issues. The overall context is health care, and the purpose of the context is both healing the patient and protecting health of the population. It can therefore be argued that in case of a global pandemic, one should allow the exchange of patient's data, especially when it comes to data about infected patients and their contacts, to the extent that it is necessary to manage the pandemic.

There is, however, a danger of misusing the collected data outside of the defined context – the so-called "mission creep", which experts argue was the case with NSA collecting data from both US and foreign citizens on an unprecedented scale as an aftermath of the 9/11 terrorist attack [16]. Furthermore, aside from the danger of collecting data by the government, the crisis situation leads to increase of data collection by private companies, as people all over the world switch to remote communication and remote collaboration tools from face-to-face communications. The privacy policies of these tools are likely to be too long, obscure, and complicated to figure out and the important details might consequently be ignored by the users of these tools. Moreover, even among the privacy-concerned users, the adoption of more privacy-friendly tools can be hindered by social pressure and network effects, if everyone else prefers to use more popular tools that are less inclined to protect the privacy of their users. This data collection even furthers the effects of the so-called *surveillance capitalism* [17], which leads to corporations having even more power over people than before the crisis. This access to personal data by corporations is furthermore aggravated by an increased usage of social media platforms, increases in users sharing their location data and giving applications increased access to their phone's operating system. Lowered barriers and increased online activity that can be directly linked to an individual or an email address is a treasure trove for for-profit corporations that monetize consumer data. Many corporations are now getting free or low cost leads for months to come.

A question that is often open for discussion is to which extent people themselves would be ready to share their data, even if it results in a privacy loss. As such, data sharing habits in general have been the topic of research, leading to discussions on so-called privacy paradox: people claiming that privacy is important to them, yet not behaving in a privacy-preserving way. The privacy paradox can be explained by different factors [18]. One of them is the lack of awareness about the extent of data collection as well as about the possible harms that can result from unrestricted data sharing. A further factor stems from decision biases, such as people's tendency

to underestimate the risks that may happen in the future compared against immediate benefit. Another noteworthy factor are the manipulations by service providers (so-called dark patterns) nudging users into sharing more of their data contrary to their actual preferences. But rational decisions in times of crisis are even more difficult. Given the state of stress and anxiety many are in, people might be more likely to accept privacy-problematic practices if they are told that these practices are absolutely necessary for managing the crisis – even if this is not actually the case.

The problem that people are more likely to surrender their privacy rights if they have already had to surrender other basic rights (such as freedom of movement due to lockdown restrictions) is reminiscent of the psychological mechanism of door-in-the-face technique. The door-in-the-face technique is a method of social influence, where a person at first is asked to do something that requires more than he or she would accept, they are more likely to accept further smaller favors afterwards [19]. In case of the SARS-CoV-2 pandemic, the big request (e.g. the restriction of fundamental personal rights, which one would not agree to under normal circumstances) is followed by the question of an apparently smaller favor (e.g. the acceptance of private data use), the smaller favor is fulfilled with a higher willingness. But according to Cantarero et al. the level of acceptance differs from individual to individual [20], which makes it even more important to rise consciousness in population.

At the same time, timely access to data voluntarily shared by people (in addition to the data collected by hospitals and authorities) can indeed be helpful in combating the epidemics. In this, supporting informed consent of data subjects, ensuring their trust in the institutions with whom the data is shared and implementing of appropriate measures to secure the collected data serve as safeguards against privacy harms.

D. Information Security Concerns

In an increasingly digital world, establishing proper information security safeguards is critical in preventing data leaks, and hence, in preserving privacy of data subjects. Yet, the situation of such a global pandemic places significant challenges on established workflows, information technology and their security as well, resulting in various issues.

A large amount of these issues are related to the fact that employees are forced to work from home and that travel becomes restricted. While some companies and institutions have provided a possibility for remote work also before the crisis, or are at least infrastructurally and organizationally prepared, many are unprepared to such a dramatic increase of home office work. The latter companies are faced with significant technical and organizational challenges, such as ensuring security of the system given the need for opening the network to remote access, e.g. via the so-called demilitarized zone (DMZ), or perimeter control, extension of technical monitoring of the system and overall extension of system hardening in ”hostile” (home) environments. A recent poll revealed that the security teams of 47% of companies did not have ”emergency plans in place to shift an on-premise workforce to one that is remote” [21]. Even worse, these challenges are more present in regulated (and therefore often critical) industries as Sumir Karayi, CEO and founder of 1E, in an Threatpost interview states:

“Government, legal, insurance, banking and healthcare are all great examples of industries that are not prepared for this massive influx of remote workers [...] Many companies and organizations in these industries are working on legacy systems and are using software that is not patched. Not only does this mean remote work is a security concern, but it makes working a negative, unproductive experience for the employee. [...] Regulated industries pose a significant challenge because they use systems, devices or people not yet approved for remote work [...] Proprietary or specific software is usually also legacy software. It’s hard to patch and maintain, and rarely able to be accessed remotely.“ [22]

In consequence, the urgent need to enable remote collaboration related with the lack of preparation and preparation time may lead to hurried and immature remote work strategies.

At the same time, ensuring proper security behaviour of the employees – something that was a challenge in many companies also before the crisis – is becoming an even more difficult task. Not only do we currently see an increase in coping strategies on an employee-base, i.e. employees try to circumvent corporate restrictions by sending or sharing data and documents over private accounts (the so-called shadow IT); but furthermore, that there has been a surge of social engineering attacks, among other phishing email campaigns, business email compromise, malware and ransomware strains, as Sherrod DeGrippo, senior director of threat research and detection at Proofpoint, states [23].

Similar findings are provided by Atlas VPN research, which shows that a number of industries broadly use unpatched or no longer supported hardware or software systems, including healthcare sector [24].

Together with immature remote strategies, information security and privacy risks may significantly increase and undermine the standardized risk management process.

E. General Data Protection Regulation (GDPR) in Context of the Pandemic

The European Data Protection Board (EDPB) has formulated a statement on the processing of personal data in the context of the SARS-CoV-2 outbreak [25].

According to EDPB, data protection rules do not hinder measures taken in the fight against the coronavirus pandemic. Even so, the EDPB underlines that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects.

Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data and in this context one must respect the general principles of law. As such, the GDPR allows competent public health authorities (e.g. hospitals, laboratories, etc.) and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein.

With regard to the processing of telecommunication data, such as location data, the national laws implementing the ePrivacy Directive must also be respected. The national laws implementing the ePrivacy Directive provide that the location data can only be used by the operator when they are made anonymous, or with the consent of the individuals. If it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the member states to introduce legislative measures pursuing national security and public security.

This emergency legislation is possible under the condition that it constitutes a necessary, appropriate and proportionate measure within a democratic society. If such measures are introduced, a member state is obliged to put in place adequate safeguards, such as granting individuals the right to judicial remedy.

III. Robert Koch Institute and Telekom Case

In this section we conduct a preliminary analysis of German disease control receiving movement data from a telecommunication provider.

In Germany, the authority for disease control and prevention, the Robert Koch Institute (RKI), made headlines on March 18 2020, when it became public that telecommunication provider Telekom had shared an anonymized set of mobile phone movement data to monitor citizens' mobility in relation to the spread of SARS-CoV-2. 46 million Telekom customers' data was sent to the RKI for further analysis. The German Federal Commissioner for Data Protection and Freedom of Information, Ulrich Kelber, overseeing the transfer, commented on the incident that he's not concerned about violating any data protection rules, as the data had been anonymized upfront [26].

However, it has been shown in the past that seemly anonymized data sets can indeed be "deanonymized" [27]. Constanze Kurz, an activist and expert on the subject matter, commented that she was skeptical about the anonymization. She urged Telekom to publicize the anonymization methods that were being used and asked the Robert Koch Institute to explain how this data will be protected from third parties in the future. Indeed, several research studies show how seemingly-anonymized data can be deanonymized and personal information about data subjects reconstructed. That includes a case that was brought up to people's attention in 2016, when a journalist and a data scientist acquired an anonymized dataset with the browsing habits of more than three million German citizens [28], [29].

As at the moment it is hard to tell whether disclosure of personal data is possible from the shared set (even more so given the development of new re-identification methods, including possible future development), we look at the worst-case scenario, namely, that personal data can indeed be reconstructed. Given this scenario, we use Nissenbaum's contextual integrity thesis to understand if privacy was still preserved in this context [14]. We do so by stating the context of the case, the norm – what everyone expects should happen – plus five contextual parameters to further analyze the situation. The table I below summarises the contextual integrity framework as applied to the German data sharing situation.

Table I
Nissenbaum's contextual integrity applied to the Robert Koch Institute and Telekom case.

Parameters	Contextual information
Context	Health care, including public health
Norm	The Robert Koch Institute is responsible to prevent the spread of disease in Germany and is currently fighting further spread of SARS-CoV-2
Data Subjects	46 million customers of German Telekom
Sender	German Telekom or subsidiary Motionlogic
Recipient	The Robert Koch Institute
Information type	Mobile phone movement data
Transmission principle	Sender and Recipient are working with the German Federal Commissioner for Data Protection and Freedom of Information to ensure that the shared data was anonymized and is only used to prevent the spread of SARS-CoV-2 in Germany

A principle that is perhaps most interesting for further elaboration is the transmission principle. Given the context and urgency of the situation, one might agree that having the German Federal Commissioner for Data Protection and Freedom of Information oversee the transaction and taking some measures to anonymize the data set appropriately serves as a practical solution towards limiting the spread of SARS-CoV-2, also without explicitly obtaining consent from data subjects. We do, however, assume that appropriate use of data would be limiting it to a specific purpose of combating the pandemic, and not reusing it to other purposes without further assessment. Note, however, that there is space for discussion, in which the community should be engaged, about the norms that apply in this situation, especially given the extraordinary situation and the severity of the crisis.

A further step of the contextual integrity is, however, also part of the contextual integrity framework to Nissenbaum's five parameter thesis of contextual information to create hypothetical scenarios that could imbalance decision's future integrity. We therefore consider the following hypotheticals which we believe would violate contextual integrity:

Hypothetical scenario 1: "The Robert Koch Institute does not delete the data after SARS-CoV-2 crisis"

Hypothetical scenario 2: "The Robert Koch Institute forwards data to other state organs or to third parties"

Hypothetical scenario 3: "The Robert Koch Institute uses data for other purposes different from fighting SARS-CoV-2 spread or other similar public health crises"

These hypothetical scenarios would violate the transmission principle that the data will only be used for handling the crisis (and, in the second hypothetical, also the receiver of the data). In case of these changes, another assessment would be essential to determine whether the transfer is justified by

the need to fight the pandemic or whether new permissions such as customer consent are required.

Hypothetical scenario 4: "The Robert Koch Institute requests data about phone calls and text messages exchanged by Telekoms' customers

Hypothetical scenario 5: "The Robert Koch Institute requests data about Telekom customer movements from the last ten years

In these scenarios , the information type is changed, and it can be argued that the new exchanged data no longer serves the purpose of fighting the pandemic. This point was also made by the Electronic Freedom Frontier organisation [30], noting that since the incubation period of the virus is estimated to last 14 days, getting access to data that is much older than that would be a privacy violation. Same as with the first three scenarios, a further assessment needs to be made and transparent information and consent request policies should apply.

Hypothetical 6: "The Robert Koch Institute uses the data purely for fighting SARS-CoV-2, but fails to keep it secure against hackers."

As with the first three scenarios, the transmission principle of confidentiality is violated in this scenario, albeit unintentionally, and, in case of improper anonymization, personal information might still be leaked. Hence, a privacy violation has taken place. Therefore, appropriate protection measures should be implemented.

IV. Recommendations and Outlook

Numerous initiatives have been taken to slow down the spread of the SARS-CoV-2 such as remote working, telemedicine, and online learning and shopping. This has required a legion of changes in our lives. However, as mentioned in previous sections, these activities come with associated security and privacy risks, and concerns have been raised regarding these risks (see e.g. the statement and proposed principles from the Electronic Freedom Frontier [30].

Of particular interest is the case of healthcare systems, which must be transparent with the information related to patients, but cautious with the disclosed information. Equally, hospitals might also decide to withhold information in order to try to minimize liability. This is a slippery slope: both cases – no information or too much information – might lead to a state of fear in the population and a false sense of security (i.e. no information means there is no problem) or a loss of privacy when too much information is disclosed.

In the current situation and others that might arise, principles and best practices developed before the crisis are still applicable. Namely, privacy by design principles, and most importantly, data minimisation. Only strictly necessary data needed to manage the crisis should be collected, which must be subsequently deleted once the crisis is contained and it is no longer needed.

In this context, patient data should be collected, stored, analysed and processed under strict data protection rules (such as the General Data Protection Regulation GDPR) by competent public health authorities as mentioned in the previous chapter.[reference link] An example of addressing the issues of data protection during the crisis can also be seen within the Austrian project VKT-GOEPL [31]. The goal of the project was to generate a dynamic situational map in case of a crisis for stakeholders, such as ministries. Events, such as terrorist attacks, flooding, fire and pandemic scenarios were selected. Already ten years ago the need of geographical, movement data provided by telecommunication providers was treated as a use-cases. Furthermore, the linking of personal data from different databases was prohibited in cases where this data was not anonymized. In all circumstances, individuals must be transparently informed about the policies which apply to the processing of their personal data.

Regarding data analysis, personal data should only be disclosed to authorised parties after adequate security measures and confidentiality policies are adopted. Moreover, only data which is strictly necessary should be shared. Proper data storage should be ensured by using advanced technology such as cryptography. Patient data – including personal information such as contact data, sexual preferences or religion amongst others – should not be revealed. Partial or total anonymization of the metadata contained in the patient history should be carried out prior to sharing.

In addition, to ensure privacy from the collection stage, consistent training of the medical personnel, volunteers and administrative staff should be done. The current lack of training (due to limited resources, shortage of specialists and general time pressure) leads to human errors and neglect of proper security and privacy protection measures.

A further concern, which is not investigated in details in this paper, is ensuring fairness when it comes to algorithmical decision making. As such, automated data systems ("big data" or "machine learning") are known to have issues with bias based e.g. on race or gender that can lead to discrimination [32]. In order to prevent such adverse effects during the crisis, these systems should furthermore be limited in order to limit bias based on nationality, sexual preferences, religion, or other factors that are not related to handling the pandemic.

Finally, we recognize that having access to timely and accurate data can play a critical role in combating the epidemic. Yet, as discussed in previous sections, ignoring issues around collection and handling of personal data might cause serious harm that will be hard to repair in the long run. Therefore, as data is being collected from the population, it is of crucial importance that this data is handled responsibly and keeping the privacy of the data subjects in mind.

References

[1] L. S. Fischer, S. Santibanez, R. J. Hatchett, D. B. Jernigan, L. A. Meyers, P. G. Thorpe, and M. I. Meltzer, "Cdc grand rounds: Modeling and public health decision-making," *Morbidity and Mortality Weekly Report*, vol. 65, no. 48, pp. 1374–1377, 2016. [Online]. Available: https://www.jstor.org/stable/24859189

[2] S. K. Brooks, R. K. Webster, L. E. Smith, L. Woodland, P. S. Wessely, P. N. Greenberg, and G. J. Rubin, "The psychological impact of quarantine and how to reduce it: rapid review of the evidence," *Lancet*, vol. 65, no. 395, pp. 912–20, February 2020. [Online]. Available: https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)30460-8/fulltext

[3] N. M. Ferguson, D. Laydon, G. Nedjati-Gilani, N. Imai, K. Ainslie, M. Baguelin, S. Bhatia, A. Boonyasiri, Z. Cucunubá, G. Cuomo-Dannenburg, A. Dighe, I. Dorigatti, H. Fu, K. Gaythorpe, W. Green, A. Hamlet, W. Hinsley, L. C. Okell, S. van Elsland, H. Thompson, R. Verity, E. Volz, H. Wang, Y. Wang, P. G. Walker, C. Walters, P. Winskill, C. Whittaker, C. A. Donnelly, S. Riley, and A. C. Ghani, "Impact of non-pharmaceutical interventions (npis) to reduce covid-19 mortality and healthcare demand," *Imperial College COVID-19 Response Team*, 2020. [Online]. Available: https://www.imperial.ac.uk/media/imperial-college/medicine/sph/ide/gida-fellowships/Imperial-College-COVID19-NPI-modelling-16-03-2020.pdf

[4] J. W. Sonn, "Coronavirus: South korea's success in controlling disease is due to its acceptance of surveillance," March 2020, [Online; posted 22-Marc-2020]. [Online]. Available: https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068

[5] V. J. Lee, C. J. Chiew, and W. X. Khong, "Interrupting transmission of COVID-19: lessons from containment efforts in Singapore," *Journal of Travel Medicine*, 03 2020, taaa039. [Online]. Available: https://doi.org/10.1093/jtm/taaa039

[6] S. Lai, N. W. Ruktanonchai, L. Zhou, O. Prosper, W. Luo, J. R. Floyd, A. Wesolowski, M. Santillana, C. Zhang, X. Du, H. Yu, and A. J. Tatem, "Effect of non-pharmaceutical interventions for containing the covid-19 outbreak in china," *medRxiv*, 2020. [Online]. Available: https://www.medrxiv.org/content/early/2020/03/13/2020.03.03.20029843

[7] O. Holmes. (2020) Israel to track mobile phones of suspected coronavirus cases. [Online]. Available: https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases

[8] D. Estrin. (2020) Israel begins tracking and texting those possibly exposed to the coronavirus. [Online]. Available: https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus?t=1584807584909

[9] J. A. Gross and T. Staff. (2020) Israel starts surveilling virus carriers, sends 400 who were nearby to isolation. [Online]. Available: https://www.timesofisrael.com/health-ministry-begins-controversial-tracking-of-coronavirus-patients/

[10] M. Sulzbacher and M. Al-Youssef. (2020) Mobilfunker a1 liefert bewegungsströme von handynutzern an regierung. [Online]. Available: https://www.derstandard.at/story/2000115828957/mobilfunker-a1-liefert-bewegungsstroeme-von-handynutzern-der-regierung

[11] C. Troncoso, *"Privacy Online Rights", The Cyber Security Body of Knowledge*, Aug 2019.

[12] Arendt, *The Human Condition*. Chicago, IL: University of Chicago Press, 1958.

[13] H. Nissenbaum, *Privacy as contextual integrity*, 2004.

[14] ——, *Contextual Integrity Up and Down the Data Food Chain*. Theoretical Inquiries Law, 2019.

[15] C. Cadwalladr. (2020) Fresh cambridge analytica leak 'shows global manipulation is out of control'. [Online]. Available: https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation

[16] B. Schneier. (2013) Mission creep: When everything is terrorism. [Online]. Available: https://www.schneier.com/essays/archives/2013/07/mission_creep_when_e.html

[17] S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology*, 04 2015. [Online]. Available: https://ssrn.com/abstract=2594754

[18] D. J. Solove, "The myth of the privacy paradox," *Available at SSRN*, 2020.

[19] K. Moser, "Door-in-the-face-technik," in *Dorsch Lexikon der Psychologie*, M. A. Wirtz, Ed. Verlag Hans Huber, 2013, p. 364.

[20] K. Cantarero, M. Gamian-Wilk, and D. Dolinski, "Being inconsistent and compliant: The moderating role of the preference for consistency in the door-in-the-face technique," *Personality and Individual Differences*, vol. 115, 2015.

[21] T. Seals. (2020) Coronavirus poll results: Cyberattacks ramp up, wfh prep uneven. [Online]. Available: https://threatpost.com/coronavirus-poll-cyberattacks-work-from-home/153958/

[22] ——. (2020) Working from home: Covid-19's constellation of security challenges. [Online]. Available: https://threatpost.com/coronavirus-poll-cyberattacks-work-from-home/153958/

[23] A. Scroxton. (2020) Coronavirus now possibly largest-ever cyber security threat. [Online]. Available: https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat

[24] (2020) Us is fighting covid-19 with 83outdated software. [Online]. Available: https://atlasvpn.com/blog/us-is-fighting-covid-19-with-83-percent-of-healthcare-systems-running-on-outdated-software/

[25] EU. (2020) Statement onthe processing of personal data in the context of the covid-19outbreak. [Online]. Available: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[26] M. Balser and S. Hurtz. (2020) Warum die Telekom Bewegungsdaten von Handynutzern weitergibt. [Online]. Available: https://www.sueddeutsche.de/digital/coronavirus-telekom-smartphone-tracking-datenschutz-1.4850094

[27] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review*, vol. 57, 2010.

[28] L. Rocher, J. Hendrickx, and Y. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Commun*, 2019. [Online]. Available: https://www.nature.com/articles/s41467-019-10933-3

[29] M. J. Khan, CISA, CRISC, and C. andGlobal Audit Head, "Big data deidentification, reidentification and anonymization," *ISACA Journal*, 2018. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization

[30] M. Guariglia and A. Schwartz. (2020) Protecting civil liberties during a public health crisis. [Online]. Available: https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis

[31] C. Flachberger and J. Prinz. Crisis and disaster management as a network-activity. [Online]. Available: https://episecc.eu/sites/default/files/1569928929%20ih_updated.pdf

[32] C. O'Neill, "Weapons of math destruction," *How Big Data Increases Inequality and Threatens Democracy*, 2016.