Government Surveillance Amid the Covid-19 Pandemic: Contact Tracing Apps and Issues of Data Privacy

Sofia Bordin Rolim
Law graduate (Pontifícia Universidade Católica do Rio Grande do Sul) and public servant at Tribunal de Contas do Município de São Paulo (Audit Court of the City of São Paulo)

Abstract: This article aims to examine the use of contact tracing apps during the COVID-19 pandemic in a context of rising government surveillance and digital authoritarianism. Through a data protection perspective, we will consider key attributes of these softwares such as system architecture and data management, and examine their main privacy implications. We briefly explore some of the surveillance methods employed around the world and reflect on its implications for individual freedoms and democracy. At last, we examine the findings of a systematic review of the effectiveness of automated contact-tracing for preventing the spread of the novel coronavirus.

Keywords: Data protection. Government surveillance. Contact tracing. Privacy. Digital authoritarianism.

1 Why data matters: surveillance and digital authoritarianism

In 2018, the Cambridge Analytica (CA) data scandal revealed how, through Facebook, the company had been harvesting user data without their consent, and using it to influence voter preference and election results. An app owned by CA was offered on the social media platform to thousands of users, who were paid to complete an online survey and consented on having their data collected for

"academic purposes". Although Facebook's platform policy prohibits the collection of users' friends' data for commercial or advertising purposes,[1] CA was able to gather data from 87 million Facebook users, albeit only 270 thousand people had downloaded the app.[2] This information was then used for *online political microtargeting* which, by removing the political debate from the public sphere, poses a threat of manipulation as well as voter suppression, and facilitates the spread of misinformation.[3] The Cambridge Analytica case shone light not just on this one instance of illegal data harvesting and its political use, but on how little control and knowledge governments and civil society have over the way private companies collect, store and share citizens' data.

The debate on how "Big Tech" – the dominant companies in the information technology sector, often referred to as "Big Four/Five" in reference to Amazon, Google, Facebook, Apple, and sometimes Microsoft – benefit economically and even structure their business model on the user data they aggressively collect, often without appropriate consent, has been ongoing among privacy law experts, digital rights activists, political philosophers and social scientists concerned about democratic decline, and even liberal economists, entrepreneurs and lawyers who advocate for breaking up the Big Four on the grounds of how monopoly stifles innovation and competition.[4] For Harvard Business School professor Shoshana Zuboff, the contemporary approach of Big Tech and private enterprise towards user data has instituted a "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales"[5] she labels *surveillance capitalism*. Zuboff unravels how, through machine intelligence, data is used to fabricate extremely lucrative *prediction products* – that is, predictions of future user behaviour. In the competitive search for ever-more-predictive behavioural data, companies have realized the efficiency of nudging consumer behaviour into more profitable outcomes. This has produced a shift "in which automated machine processes not only *know* our behavior but also *shape* our behavior at scale"[6].

Furthermore, the threat of the use of digital surveillance in order to track and suppress political dissidents – known as *digital authoritarianism* – is present throughout the democracy spectrum.[7] According to Freedom House, the COVID-19 pandemic has accelerated an already sharp process of decline in internet freedom across the world:

> [...] authorities cited COVID-19 to justify expanded surveillance powers and the deployment of new technologies that were once seen as too intrusive. The public health crisis has created an opening for the digitization, collection, and analysis of people's most intimate data without adequate protections against abuses. Governments and private entities are ramping up their use of artificial intelligence (AI), biometric surveillance, and big-data tools to make decisions that affect individuals' economic, social, and political rights. Crucially, the processes involved have often lacked transparency, independent oversight, and avenues for redress. These practices raise the prospect of a dystopian future in which private companies, security agencies, and cybercriminals enjoy easy access not only to sensitive information about the places we visit and the items we purchase, but also to our medical histories, facial and voice patterns, and even our genetic codes.[8]

In the following topics, we will address how this process of increased surveillance and data collection has played out in regards specifically to the development and promotion of apps relying on GPS monitoring in order to track cases of potential exposure to the SARS-CoV-2 virus.

2 The emergence of COVID-19 and contact tracing

In December 2019, doctors and medical researchers based in Wuhan, capital of the central chinese Hubei province, were hustling to identify the origin of the pneumonia-like disease which had quickly infected dozens of the city's residents.[9] On January 3rd, 2020, the National Institute of Viral Disease Control and Prevention identified the first complete genome of the virus subsequently designated as SARS-CoV-2[10] on a patient's fluid samples[11]; 16 days later, there were 198 confirmed cases in Wuhan, with reported cases in Japan, South Korea, Thailand, and elsewhere in China.[12] On January 30th, 2020, when virus patients had been diagnosed in 18 countries outside China, the World Health Organization (WHO) declared the novel coronavirus outbreak a public health emergency of international concern under the International Health Regulations.[13]

By January 5st, 121 close contacts of the infected patients had been identified and placed under medical observation;[14] before the end of the month, Wuhan had been placed under a strict lockdown, and completely isolated from the rest of the country.[15] As more information on the virus and its disease were uncovered, rapid case identification and contact tracing quickly became key strategies for public health response. With a mean incubation period of 3 to 9 days[16] and evidence of pre-symptomatic transmission,[17] isolating potentially infected individuals before they went on to further spread the disease became a complex challenge for public health officials and governments worldwide.

The challenges of "analogic" contact tracing are plenty. First and foremost, the process of conducting individual interviews is time consuming and, in contexts where the daily caseload is on the rise, can quickly overwhelm health officials. Secondly, the information provided by the interviewees on the places they have visited and the people they have come in contact with within a certain time frame is subject to inaccuracies due to memory lapses.[18] At last, for various reasons, people may lie or omit information on their whereabouts and encounters, or may not wish to come forward and undergo a contact tracing interview. South Korea was confronted with this challenge in May 2020, when a virus outbreak in bars and clubs known to cater to the LGBTQ+ population in the bohemian district of Itaewon, in Seoul, infected over 200 people[19]. Due to the stigma faced by this community, many were unwilling to report that they had attended the nightlife establishments and get tested, for fears of having their sexuality outed to the public. The mayor of Seoul guaranteed anonymity for all those seeking testing in connection to the Itaewon cluster, but apprehensiveness over privacy breaches remained.[20]

The importance of the rapid detection of new cases in the early moments of an outbreak order to prevent small-scale clusters from evolving into a scenario of sustained community transmission was becoming increasingly clear. According to the WHO, "surveillance, rapid response teams, and case investigation" is one of the main pillars in COVID-19 preparedness and response planning.[21] While thousands of workers were hired to to work full time in contact tracing,[22] many countries have also resorted to technology and surveillance for the solution. Contact tracing apps developed for smartphones will track their users' location and alert them when they have come in close contact with someone infected by the virus; thus, potentially exposed individuals can rapidly seek testing and prevent further contagion.

3 Key features of contact tracing apps and privacy aspects

Contact tracing apps have now been launched by dozens of countries around the world, with varied architectures and approaches to data privacy, and while most attempt to encourage citizens to install the softwares, more authoritarian-inclined governments have made their usage mandatory. The main privacy considerations rotate around concerns over the access

which third parties may gain to citizens' Personally Identifiable Information (PII) and location, and how this data can be used by governments for purposes other than epidemiological control, or once the pandemic is over. We will approach selected aspects of system architecture and data management in order to address possible implications for user privacy.

The essence of digital contact tracing is *location data*, which may be collected through a number of different technologies which can be used to infer the user's absolute or relative location. Systems based on absolute location data (gathered through GPS location, WiFi access points, or cell towers) monitor users' movement constantly and are widely deemed to be more intrusive in terms of personal privacy; however, although they offer a broad view on the mobility patterns of individuals, the generated data may not be sufficiently precise to determine epidemiological close contact proximity. On the other hand, relative location data obtained through the pairing of two devices with Bluetooth technology can offer more precise information, but would require that a large percentage of the population install the application in order to be effective.[23] Also, distance estimation may vary depending on the power level of the transmission of the Bluetooth signal, which varies in different phones, while the transmission patterns from the same device may be affected by the use of a phone case or the orientation of the phone's antenna.[24] On the efficiency of contact-tracing apps in regards to proximity estimation, Ahmed *et al* concluded that

> Claims of "guaranteed" accuracy of order 1m by any current app should therefore be considered with some scepticism. [...] with the techniques used by current apps for proximity estimation, there would still be many false positives and false negatives. The proximity estimate may indicate close contact, whereas the actual contact is far off or erroneously indicates that it is far off when it is nearby. Similarly, a close contact as perceived by distance estimation does not always translate into an exposed case as there may be a wall/obstruction between the two individuals (e.g., two adjacent apartments), or the contact has occurred in open space where chances of infection are lower. However, getting false positives is not as disastrous, as they only result in additional tests for these false cases. False negatives are a more significant issue as these are considered a missed opportunity to register contact with a positive case.[25]

The types of system architecture more commonly adopted for the collection of this data are the centralized, decentralized, and hybrid approaches, which we will briefly explore. The main feature of the centralized architecture is the central server which stores encrypted PII information, generates privacy-preserving temporary identifications (TempID) for each registered device, performs risk analysis, and notifies close contacts of an infected individual.[26] Therefore, data stored by the central server includes users' personal information such as name, phone number, age range and ZIP code, as well as users' TempIDs, and contact details for positive cases and close contacts of each of the positive cases.[27] An attack on the server, therefore, could jeopardize the privacy of all users and their respective contacts.[28]

The decentralized architecture aims to prevent data leaks by avoiding the accumulation of responsibilities on a single server. In this model, the attributions are moved to the user's personal device, which will generate an anonymous identifier and process the exposure notifications and risk analysis.[29] In this scenario, the only data stored by the server are the seeds voluntarily uploaded by users diagnosed with the virus.[30] Smartphones, however, tend to be less secure than a server, and the user is vulnerable to having the device stolen, or being coerced into granting a third party access to the stored data. Also, malicious attacks could succeed at de-anonymised users' personal information and identify COVID-19-positive users by downloading the seeds uploaded to the server, if the attackers gained access to data collected from

side-channel context information[31].

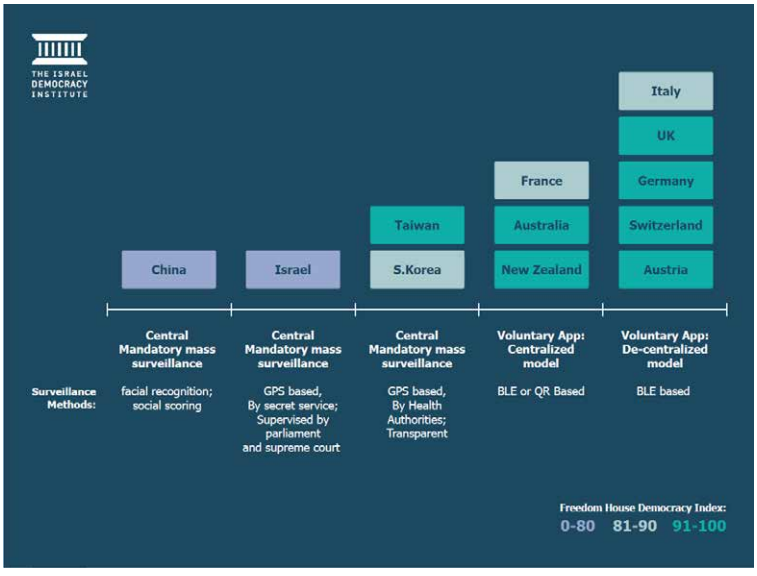
At last, the hybrid model shares the tasks between server and user device: while the generation and management of temporary identifiers remain decentralised, the tracing process itself (that is, risk analysis and notification) is performed by the server.[32] Data stored by the server includes device ID, Private Encounter Tokens voluntarily received from positive cases, metadata from positive cases, and Private Encounter Tokens uploaded from other users e for a risk analysis to be carried out by the server.[33] The de-anonymization risk encountered in the hybrid systems "adopt additional advanced privacy enhancement methods such as secret sharing, decisional Diffie-Hellman (DDH), and private set intersection"[34].

Contact tracing apps currently being developed or already at use in different countries have made a range of choices in regard to system architecture and other features. Apps such as *TraceTogether*, deployed by the Singaporean government; *CovidSafe*, launched by the government of Australia; the French *Stop-Covid* app; and *Aarogya Setu*, which collects both absolute and relative data and whose download has been made mandatory by the Indian government for certain segments of the population,[35] are all based on centralized architecture.[36] On the other hand, the exposure notification system developed by Apple and Google adopts a decentralised model, as does the Israeli *HaMagen* app.[37] Another relevant issue is the lack of transparency verified in the vast majority of currently active contact tracing apps, for which Ahmed *et al.* suggest two main approaches. Firstly, the app's source code should be open, and subjected to periodic reviews and trusted third-party audits, and secondly, the carrying out of Privacy Impact Assessment should be a basic requirement for all functioning apps.[38]

4 Surveillance methods and threats to user privacy

Although any kind of data collection and storage will pose *some* degree of risk to data privacy and individual liberties due to the impossibility of fully eliminating threats of leaks, malicious attacks or misuse, the surveillance tools employed by some countries evidently exceed the amount of monitoring required for epidemiological purposes. Below, we reproduce a chart produced by Tehilla Shwartz Altshuler and Rachel Aridor Hershkovitz, researchers at the Israel Democracy Institute, which lists a variety of surveillance methods, ranked from more intrusive to less, adopted by various countries, pointing out how these states rank in the Freedom House Democracy Index.

Figure 1 - Freedom House Democracy Index



Source: Israel Democracy Institute[39]

The chart ranged from central mandatory mass surveillance in China, where telecom providers share user data with authorities and facial recognition cameras identify pedestrians and measure their body temperature from a distance, until decentralized apps developed by European states, more strictly bound by data protection law, where location data collection should be bound by consent or anonymization.[40] South Korea and Taiwan, despite being relatively well-ranked by Freedom House, have deployed extensive surveillance methods and collected location data in a mandatory fashion. Previous experience with epidemics such as SARS and swine flu left a legacy of epidemic-specific legislation, which, in Taiwan, "authorizes the healthcare service to conduct broad epidemiological studies, and impose sanctions on those who refuse to cooperate with it"[41] and " permits people to refuse to take part in an epidemiological investigation, but [subjects them] to sanctions if this refusal cannot be justified"[42] in South Korea. In regards to the Chinese mass surveillance system, philosopher Byung-Chul Han notes:

> Critical awareness of digital surveillance is practically non-existent in Asia. There is almost no talk of data protection, including liberal states like Japan and Korea. No one is irritated by the authorities' frenzy to collect data. Meanwhile, China has introduced a system of social credit unimaginable to Europeans, which allows people to be assessed and exhaustively evaluated. Each must be assessed as a result of their social conduct. In China, there is no moment in everyday life that is not subject to observation. Each click, each purchase, each contact, each activity on social networks is controlled. Whoever crosses the red light, whoever has contact with critics of the regime and whoever makes critical comments on social networks loses points. Life, then, can become very dangerous. On the contrary, those who buy healthy food online and read newspapers that support the regime earn points. Those who have enough points get a travel visa and cheap credits. On the contrary, those who fall below a certain number of points may lose their job. In China, this social surveillance is possible because there is an unrestricted exchange of data between Internet and cell phone providers and the authorities. There is practically no data protection. In the Chinese vocabulary there is no term for "private sphere".[43] (Translation our own)

In Israel, although the previously mentioned *HaMagen* app is offered for download on a voluntary basis, the country has deployed its domestic security service, Shin Bet, to track and monitor the location of individuals without their consent in order to curb virus contagion. The contact-tracing program, which relies on cellphone surveillance, was halted by the country's High Court in April 2020 after identifying severe violations to privacy rights[44]; although the Israeli government argued that the emergency measures were necessary, and that an app would be useless to track the country's ultra-Orthodox community, who don't own smartphones, the legal ruling determined that a privacy-compliant alternative should be sought.[45] Two months later, the Knesset, Israel's Parliament, passed a law authorizing Shin Bet to continue tracking.[46] The country lacks modern privacy protection legislation and has an " inherent tendency" of resorting to security forces in emergency situations[47], which increases the threat government surveillance poses to individual liberties. Among the assessed countries, intelligence agencies were involved in data collection and tracking in Israel and China only.[48]

Altshuler and Hershkovitz reflect on the motivations and consequences of the mass surveillance employed by Israel and other countries with authoritarian tendencies:

> Countries such as China and Russia saw the pandemic as a golden opportunity to expand

> the state's coercive powers over citizens and to use technology in order to identify, track, acquire knowledge, and intimidate. When the pandemic dies down, they will find some other excuse, and the heightened surveillance will continue. In Israel, too, the decision-makers' obstinate insistence on continued use of the GSS [General Security Service] and rejection of alternatives corroborate the claims about the slippery slope whose bottom is unpredictable. In addition, Israel finds itself in the company of illiberal democracies such as Poland, Turkey, Bulgaria, and Hungary, which exploited the coronavirus in order to strip people of their civil rights and to ignore their parliaments and courts.

Furthermore, serious security flaws and highly intrusive surveillance have been identified in other countries. A recent survey by Amnesty International has reviewed contact tracing apps from Europe, Middle East and North Africa and performed a detailed analysis on softwares from Algeria, Bahrain, France, Iceland, Israel, Kuwait, Lebanon, Norway, Qatar, Tunisia and the United Arab Emirates, ranking them on their respect for users' privacy. The international organization has highlighted the threat posed by the highly invasive surveillance tools deployed by the apps *BeAware Bahrain*, developed by the Bareinite government, *Shlonik*, deployed by Kuwait, and *Smittestopp*, Norway's official contact-tracing app, all of which track users' location in real time through GPS monitoring uploaded to a centralized server.[49] The Norwegian government has currently halted usage of *Smittestopp*.[50]

Amnesty International has also identified a serious security breach in the Qatari *EHTERAZ* app, which "would have allowed cyber attackers to access highly sensitive personal information, including the name, national ID, health status and location data of more than one million users"[51]; after the alert, the government has fixed the flaw. The organisation has criticized governments for rushing the deployment of contact-tracing apps which are "often poorly designed and lack privacy safeguards"[52], echoing concerns voiced by data privacy researchers and activists worldwide.

5 On the effectiveness of contact tracing apps

Researchers from University College London have conducted a systematic review[53] in order to assess the effectiveness of automated and partly automated contact-tracing systems in controlling the spread of COVID-19, which identified 4036 studies, 110 of which were reviewed and 15 of which were included in the final analysis and quality assessment, and was published online in August 2020. The review's primary and secondary outcomes were the number or proportion of contacts (or subsequent cases) identified, and indicators of outbreak control, uptake, resource use, cost-effectiveness and lesson learnt. In this topic, we will explore their main findings.[54]

Firstly, modelling studies have shown that the efficacy of automated contact-tracing such as the one performed by apps is dependent on two factors, the first of which is population uptake; a large percentage must download and allow such apps to collect their data – studies estimates range from 56% to 95% of the population. The second factor is timeliness of the quarantining of potentially exposed close contacts.[55] The researchers note that false positive and false negative events can be influenced by factors such as the use of personal protective equipment. ventilation levels, and separation by screens or walls unidentified by the location-monitoring technology. Further real-world data is required in order to assess the extent of the effect of these factors.[56]

Regarding the effectiveness of system architectures, Braithwaite *et al* indicate that

> Decentralised automated contact-tracing systems benefit from Apple and Google's support, meaning that interoperability

> between countries with such apps is likely to be more straightforward than between countries that use centralised systems. However, a study reported that centralised systems assess transmission risk more accurately (reducing the number of people quarantined), enable better optimisation, are less susceptible to false reports, and are more readily evaluated.[57]

The researchers refer to academic studies on the risks automated contact tracing could pose if data is breached or misused, including increased surveillance and erosion of public trust, but alert that considerations of privacy and on trade-offs between privacy and utility are not in the scope of the systematic review.

Furthermore, different studies bring up concerns over digital exclusion, although these issues are not currently well quantified. Especially in low income countries, vulnerable groups which may be more at risk of infection from COVID-19 may also be less likely to own smartphones than the general population. Contact-tracing apps would therefore be less able to reduce transmission risks in these circles, potentially amplifying their risks.[58] Although noting the scarcity of empirical studies of fully automated contact tracing, the authors have identified no empirical evidence of the effectiveness of automated contact tracing regarding identification of contacts or transmission reduction. This is not to say, of course, that contact tracing apps or other forms of automated contact tracing are *not* effective; but, merely, that its potential effectiveness has not been established as of yet.

The researchers list essential questions which should be investigated by scientists and pondered by policymakers before deploying contact-tracing apps. These issues include

> [...] whether concerns around public acceptability and privacy have been adequately addressed, with appropriate public consultation; how an automated system will be integrated with other contact-tracing and disease control strategies, in consultation with public health experts; and, perhaps most importantly, whether it is likely to be effective, cost-effective, and equitable in that context.[59]

Furthermore, if such apps or systems are deployed, it is essential that they are rigorously evaluated, "including through large-scale prospective studies of effectiveness, technical and equity dimensions", as well as "qualitative studies to improve the understanding of key social and behavioural dimensions of app use and adherence."[60]

6 Conclusion

In this article, we have examined the current context of rising government surveillance and digital authoritarianism. Shoshana Zuboff's *surveillance capitalism* helps us understand how user data and information is used not only to predict our wants and needs, but to nudge user behaviour into more profitable outcomes for private enterprise. Also, digital authoritarianism is a dangerous trend on the rise among governments, especially those with stronger authoritarian tendencies. Monitoring and surveillance is often used to curb dissent and persecute political opponents, and other technological tools are employed to predict and make policy decisions around relevant social, political and economic issues without the appropriate transparency or consent. In the context of the coronavirus pandemic, the importance of contact tracing in order to prevent virus transmission has become clear and, due to the challenges posed by manual or analogic contact tracing, governments have sought out automatized solutions. Since the automatized contact tracing process is based on location monitoring, these tools carry severe implications for user data privacy and individual liberties.

We examine key features of contact

tracing apps such as system architecture and data managing, and offering some considerations regarding effectiveness and privacy implications. The impossibility of producing a sufficiently precise proximity estimation is highlighted as a major obstacle. Relying on a study by Tehilla Shwartz Altshuler and Rachel Aridor Hershkovitz, we comment on the variety of surveillance methods employed by states holding different positions at the Freedom House Democracy Index. While tougher data privacy laws and regulations tend to discourage more intrusive surveillance in Europe, countries like China and Russia have increased vigilance and monitoring during the pandemic, intensifying threats to individual liberties and privacy. Countries like South Korea and Taiwan have also adopted mandatory surveillance methods, while Israel has resorted to its domestic security service to track and monitor its citizens' locations, despite a Supreme Court ruling which ordered the program's halt due to severe violations to privacy rights.

A systematic review conducted by researchers from University College London and published in August 2020 has examined thousands of studies on automated contact tracing in curbing the spread of COVID-19 and found no empirical evidence of its effectiveness thus far. More studies are necessary in order to better understand the impact of these policies. Any kind of location data collection and storage will pose some degree of risk to data privacy, and the hastiness with which many governments have implemented new technologies for monitoring and surveillance greatly increases these risks. We understand that further investment in automated contact tracing and its necessary surveillance and monitoring technologies should not be pursued while its effectiveness for epidemiological purposes is unclear, and the threat it poses to user privacy, individual liberties, and democratic strengthening is visible and well-documented.

References

AHMED, Nadeem; MICHELIN, Regio A.; XUE, Wanli; RUJ, Sushmita; MALANEY, Robert; KANHERE, Salil S.; SENEVIRATNE, Aruna; HU, Wen; JANICKE, Helge; JHA, Sanjay K. A Survey of COVID-19 Contact Tracing Apps. **IEEE Access**, v. 8, p. 134577 - 134601, 2020.

ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **Digital contact tracing and the coronavirus: Israeli and comparative perspectives**. Brookings. 2020a. Available at https://www.brookings.edu/wp-content/uploads/2020/08/FP_20200803_digital_contact_tracing.pdf

ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **How Israel's COVID-19 mass surveillance operation works**. Brookings. 2020b. Available at https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/

AMNESTY INTERNATIONAL. **Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.** 16 Jun 2020. Available at https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

AMNESTY INTERNATIONAL. **Norway: Halt to COVID-19 contact tracing app a major win for privacy.** 15 Jun 2020. Available at https://www.amnesty.org/en/latest/news/2020/06/norway-covid19-contact-tracing-app-privacy-win/

AMNESTY INTERNATIONAL. **Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million.** 26 May 2020. Available at https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

BORGESIUS, Frederik J. Z.;MÖLLER, Judith; KRUIKEMEIER, Sanne; Ó FATHAIGH, Ronan; IRION, Kristina; DOBBER, Tom; BODO, Balazs; DE VREESE, Claes. Online Political Microtargeting:

Promises and Threats for Democracy. **Utrecht Law Review**, v. 14, n. 1, p. 82 - 96, 2018.

BRAITHWAITE, Isobel; CALLENDER, Thomas; BULLOCK, Miriam; ALDRIDGE, Robert W. Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19. **Lancet Digital Health**, v. 2, n. 11, Nov 2020, p. 607- 621.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. The Guardian. 17 Mar 2018. Available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

GORBALENYA, Alexander E.; BAKER, Susan C.; BARIC, Ralph S. et al. The species Severe acute respiratory syndrome-related coronavirus: classifying 2019-nCoV and naming it SARS-CoV-2. **Nature Microbiology**, v. 5, n.3, p. 536–544, mar 2020.

GALLOWAY, Scott. **The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google**. New York: Random House, 2017, 448 p.

HAN, Byung-Chul. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. El País Brasil. Mar 2020. Available at https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html

HE, Xi; LAU, Eric H.Y.; WU, Peng; et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. **Nature Medicine**, v. 26, p. 672–675, Apr 2020.

HIGGINS, Julian; THOMAS, James (Eds.). **Cochrane Handbook for Systematic Reviews of Interventions**. 2nd ed., New Jersey: Wiley-Blackwell, 2019, 728 p.

KIM, Nemo. **South Korea struggles to contain new outbreak amid anti-gay backlash**. The Guardian. 11 May 2020. Available at https://www.theguardian.com/world/2020/may/11/south-korea-struggles-to-contain-new-outbreak-amid-anti-lgbt-backlash

LAPOWSKY, Issie. **Facebook Exposed 87 Million Users to Cambridge Analytica**. Wired. 4 Apr 2018. Available at https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

POLYAKOVA, Alina; MESEROLE, Chris. **Exporting digital authoritarianism: The Russian and Chinese models**. Brookings, 2019. Available at https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

PRIVACY INTERNATIONAL. **India's contact tracing app will be voluntary in theory but mandatory in practice.** Apr. 2020. Available at https://privacyinternational.org/examples/3769/indias-contact-tracing-app-will-be-voluntary-theory-mandatory-practice

PRIVACY INTERNATIONAL. **Israel's coronavirus surveillance is an example for others - of what not to do**. May 2020. Available at https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do

QIN, Amy; WANG, Vivian. **Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities**. New York Times. 24 Jan 2020. Available at https://www.nytimes.com/2020/01/22/world/asia/china-coronavirus-travel.html

SIMMONS-DUFFIN, Selena. **States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago**. NPR. 7 May 2020. Available at https://www.npr.org/sections/health-shots/2020/04/28/846736937/we-asked-all-50-states-about-their-contact-tracing-capacity-heres-what-we-learne

SIORDIA JR, Juan A. Epidemiology and clinical features of COVID-19: A review of current literature. **Journal of Clinical Virology**, v. 127, Jun 2020.

TANG, Qiang. Privacy-Preserving Contact Tracing: current solutions and open questions. **arXiv:2004.06818**, p. 1 -18, 2020.

TAN, Wenjie; ZHAO, Xiang; MA, Xuejun et al. Notes from the Field: A Novel Coronavirus Genome Identified in a Cluster of Pneumonia Cases — Wuhan, China 2019□2020. **China CDC Weekly**, v. 2, n. 2, p. 61 - 62, jan 2020.

TEACHOUT, Zephyr. **Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money**. New York: All Points Books, 2020, 320 p.

THE 2019-NCOV OUTBREAK JOINT FIELD EPIDEMIOLOGY INVESTIGATION TEAM; LI, Qun. Notes from the Field: An Outbreak of NCIP (2019-nCoV) Infection in China — Wuhan, Hubei Province, 2019-2020. **China CDC Weekly**, v. 2, n. 5, p. 79 - 80, jan 2020.

THE KOREA HERALD. **Itaewon cluster grows to 237, six-stage transmission confirmed**. 25 May 2020. Available at http://www.koreaherald.com/view.php?ud=20200525000683

TINDALE, Lauren; COOMBE, Michelle; STOCKDALE, Jessica E.; et al. Evidence for transmission of COVID-19 prior to symptom onset. **eLife**, v. 9, jun 2020

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019, 704 p.

WONG, Julia Carrie; SOLON, Olivia. **US government demands details on all visitors to anti-Trump protest website**. The Guardian, 2017. Available at https://www.theguardian.com/world/2017/aug/14/donald-trump-inauguration-protest-website-search-warrant-dreamhost

WORLD HEALTH ORGANIZATION. **Pneumonia of unknown cause – China.** 2020a. Available at https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/en/.

WORLD HEALTH ORGANIZATION. **WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)**. 2020b. Available at https://www.who.int/dg/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus-(2019-ncov).

WORLD HEALTH ORGANISATION. **COVID-19 Strategic Preparedness and Response Plan: Operational Planning Guidelines To Support Country Preparedness And Response**. 2020c. Available at https://www.who.int/docs/default-source/coronaviruse/covid-19-sprp-unct-guidelines.pdf?sfvrsn=81ff43d8_4

Notes

1 CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. 17 Mar 2018.

2 LAPOWSKY, Issie. Facebook Exposed 87 Million Users to Cambridge Analytica. Wired. 4 Apr 2018.

3 BORGESIUS, Frederik J. Z.; MÖLLER, Judith; KRUIKEMEIER, Sanne; Ó FATHAIGH, Ronan; IRION, Kristina; DOBBER, Tom; BODO, Balazs; DE VREESE, Claes. Online Political Microtargeting: Promises and Threats for Democracy. **Utrecht Law Review**, v. 14, n. 1, p. 82 - 96, 2018.

4 GALLOWAY, Scott. **The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google**. New York: Random House, 2017, 448 p. and TEACHOUT, Zephyr. **Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money**. New York: All Points Books, 2020, 320 p.

5 ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019, p. 1.

6 Ibidem, p. 8.

7 POLYAKOVA, Alina; MESEROLE, Chris. **Exporting digital authoritarianism: The Russian and Chinese models.** Brookings, 2019. and WONG, Julia Carrie; SOLON, Olivia. *U***S government demands details on all visitors to anti-Trump protest website.** The Guardian, 2017.

8 SHAHBAZ, Adrian; FUNK, Allie. **Freedom on the Net 2020: The Pandemic's Digital Shadow.** Freedom House.

9 WORLD HEALTH ORGANIZATION. **Pneumonia of unknown cause – China**. 2020a.

10 GORBALENYA, Alexander E.; BAKER, Susan C.; BARIC, Ralph S. et al. The species Severe acute respiratory syndrome-related coronavirus: classifying 2019-nCoV and naming it SARS-CoV-2. **Nature Microbiology**, v. 5, n.3, p. 536–544, mar 2020.

11 TAN, Wenjie; ZHAO, Xiang; MA, Xuejun et al. Notes from the Field: A Novel Coronavirus Genome Identified in a Cluster of Pneumonia Cases — Wuhan, China 2019□2020. **China CDC Weekly**, v. 2, n. 2, p. 61 - 62, jan 2020.

12 THE 2019-NCOV OUTBREAK JOINT FIELD EPIDEMIOLOGY INVESTIGATION TEAM; LI, Qun. Notes from the Field: An Outbreak of NCIP (2019-nCoV) Infection in China — Wuhan, Hubei Province, 2019□2020. **China CDC Weekly**, v. 2, n. 5, p. 79 - 80, jan 2020.

13 WORLD HEALTH ORGANIZATION. **WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)**. 2020b.

14 Op. cit. WORLD HEALTH ORGANIZATION, 2020a.

15 QIN, Amy; WANG, Vivian. **Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities**. New York Times. 24 Jan 2020.

16 SIORDIA JR, Juan A. Epidemiology and clinical features of COVID-19: A review of current literature. **Journal of Clinical Virology**, v. 127, Jun 2020.

17 TINDALE, Lauren; COOMBE, Michelle; STOCKDALE, Jessica E.; et al. Evidence for transmission of COVID-19 prior to symptom onset. **eLife**, v. 9, jun 2020 and HE, Xi; LAU, Eric H.Y.; WU, Peng; et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. Nature Medicine, v. 26, p. 672–675, Apr 2020.

18 AHMED, Nadeem; MICHELIN, Regio A.; XUE, Wanli; RUJ, Sushmita; MALANEY, Robert; KANHERE, Salil S.; SENEVIRATNE, Aruna; HU, Wen; JANICKE, Helge; JHA, Sanjay K. A Survey of COVID-19 Contact Tracing Apps. **IEEE Access**, v. 8, p. 134577 - 134601, 2020.

19 THE KOREA HERALD. **Itaewon cluster grows to 237, six-stage transmission confirmed**. 25 May 2020. Available at http://www.koreaherald.com/view.php?ud=20200525000683

20 KIM, Nemo. **South Korea struggles to contain new outbreak amid anti-gay backlash**. The Guardian. 11 May 2020.

21 WORLD HEALTH ORGANISATION. **COVID-19 Strategic Preparedness and Response Plan: Operational Planning Guidelines To Support Country Preparedness And Response**. 2020c.

22 SIMMONS-DUFFIN, Selena. **States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago**. NPR. 7 May 2020.

23 TANG, Qiang. Privacy-Preserving Contact Tracing: current solutions and open questions. **arXiv:2004.06818.** 2020, p. 6.

24 Op. cit. AHMED, Nadeem *et al*, p. 134586.

25 Ibid., p. 134586.

26 Op. cit. AHMED, Nadeem *et al*, p. 134584.

27 Ibid.

28 Ibid., p. 134585

29 p. 134580 - 134582

30 p. 134584

31 Ibid., p. 134585

32 p. 134580-134583

33 p. 134584

34 Ibid., p. 134585. For the referred privacy enhancement methods, see SHAMIR, A. 'How to share a secret. Commun, ACM, v. 22, n. 11, p. 612–613, Nov. 1979.; BONEH, D.'The decision diffie-hellman problem. Algorithmic Number Theory. Berlin: Springer, p. 48–63, 1998; and DE CRISTOFARO, E.; TSUDIK, G. Practical private set intersection protocols with linear complexity. Proc. Int. Conf. Financial Cryptogr. Data Secur. Springer, pp. 143–159, 2010.

35 PRIVACY INTERNATIONAL. **India's contact tracing app will be voluntary in theory but mandatory in practice**. Apr. 2020.

36 Op. cit. AHMED, Nadeem *et al*, p. 134590-134592.

37 Ibid., p. 13492 - 134594.

38 Ibid., p. 13497.

39 ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **Digital contact tracing and the coronavirus: Israeli and comparative perspectives.** Brookings. 2020a.

40 Op. cit. ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor, 2020a, p. 7.

41 Ibid, p. 8.

42 Ibid.

43 HAN, Byung-Chul. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. El País Brasil. Mar 2020.

44 PRIVACY INTERNATIONAL. **Israel's coronavirus surveillance is an example for others - of what not to do**. May 2020.

45 ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **How Israel's COVID-19 mass surveillance operation works**. Brookings. 2020b.

46 STAFF, Toi. **Knesset passes law authorizing Shin Bet tracking of virus carriers until January.** The Times of Israel. Jul 2020.

47 Op. cit. ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor, 2020a, p. 9.

48 Ibid., p. 13.

49 AMNESTY INTERNATIONAL. **Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy**. 16 Jun 2020.

50 AMNESTY INTERNATIONAL. **Norway: Halt to COVID-19 contact tracing app a major win for privac**y. 15 Jun 2020.

51 AMNESTY INTERNATIONAL. **Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million.** 26 May 2020.

52 Ibid.

53 According to the Cochrane Handbook for Systematic Reviews of Interventions (2011), systematic reviews "attempt to collate all empirical evidence that fits pre-specified eligibility criteria in order to answer a specific research question. It uses explicit, systematic methods that are selected with a view to

minimizing bias, thus providing more reliable findings from which conclusions can be drawn and decisions made."

54 BRAITHWAITE, Isobel; CALLENDER, Thomas; BULLOCK, Miriam; ALDRIDGE, Robert W. Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19. **Lancet Digital Health**, v. 2, n. 11, Nov 2020, p. 607- 621.

55 Ibid.

56 Ibid., p. 618.

57 Ibid., p. 619.

58 Ibid.

59 Ibid.

60 Ibid.