AIES

AUSTRIA INSTITUT FÜR EUROPA- UND SICHERHEITSPOLITIK

The Hague Centre for Strategic Studies

AIES-STUDIES

Dr. Alexander Klimburg, Louk Faesen, Paul Verhagen, Philipp Mirtl

Pandemic Mitigation in the Digital Age

Digital Epidemiological Measures to Combat the Coronavirus Pandemic

Nr. 12
March 2020
Vienna

AIES
Tivoligasse 73a
1120 Vienna
Austria
Tel: +43 1 3583080
office@aies.at
www.aies.at

Pandemic Mitigation in the Digital Age

Digital Epidemiological Measures to Combat the Coronavirus Pandemic

Dr. Alexander Klimburg, Louk Faesen, Paul Verhagen, Philipp Mirtl

March 28, 2020

Summary

As the current coronavirus pandemic proceeds, several governments have already utilized digital epidemiological tools to combat the spread of the SARS-CoV-2 virus, with some early successes. The role of user-based and provider-based data collection, and in particular location data, has characterized the mitigation strategies of some of the most effective national responses. These measures may impact individual privacy rights and therefore threaten to accentuate existing cognitive dissonance within public perceptions of trust in the use of surveillance tools by companies and governments alike in liberal democracies. The danger is that the public debate on the employment of these technologies may not only become excessively one-sided but will also not accurately reflect the existing technical capabilities and data-use realities of some governments, even in Europe. But an informed public debate is urgently needed.

This report recommends specific digital contact tracing and quarantine measures (CTQ) that are in accordance with existing EU legislation, and offers a way forward to consider a principle towards "data for the common good" to help combat the current coronavirus pandemic. If additional emergency legal provisions are needed to deploy further digital epidemiological measures, these should be predicated upon multistakeholder consultations, strict time limitations, and post-hoc auditability. Overall, at both national and European levels it will be necessary to engage in a wider "digital agenda for pandemic response" to deal with a threat that is not likely to be short lived, and the ramifications of which are not yet apparent.

Among the reviewed cases (Taiwan, South Korea, Singapore, China, and Israel) studied, one conclusion stands out: the more democratic nations are openly deploying existing national security means, especially in location tracking and the merging of databases. The technical recommendations proposed in this report may not be sufficient, and Europe may need to consider further-reaching measures as well. Europe has significant latent digital epidemiological capabilities within businesses and government that are often not easily apparent to the wider public, and whose technical details and relationship with personal data are often not clear. But Europe is also the single largest collection of democracies and the EU represents a historic democracy project. Not only can the state and non-state institutions of democracy handle emergency provisions, but the public at large can be expected to support them – if an informed discussion is had with the openness and accuracy it requires.

1. Recommendations – Data for the Common Good

On March 25, 2020, in an appeal for joint action against the coronavirus pandemic, United Nations Secretary General António Guterres called for immediate global ceasefire: "The fury of the virus illustrates the folly of war [..] It is time to put armed conflict on lockdown and focus together on the true fight of our lives."[1] The SARS-CoV-2 virus "threatens the whole of mankind", he said. Although Guterres was referring to physical warfare in conflict zones world-wide, his words equally hold for another needed ceasefire: namely one between excessive techno-optimism and data protection activism.

In the past weeks, dozens of nations have declared various states of emergencies and implemented public restrictions and economic support measures unprecedented since 1945. While at present there is little data as to the likely human casualties and damage to economies caused by the pandemic and its mitigation, conventional reporting indicates a European infection "peak" to be reached by May 2020. For most European Union (EU) Member States, there is a possibility that, after the current "crisis", similar infection peaks and therefore new crises may occur in the fall or spring of next year, even if SARS-CoV-2 "herd immunity" is reached. Therefore the "emergency", "exceptional", or "alarm state" is likely to continue for the near future across Europe.

Contact tracing and quarantine (CTQ) technologies have been directly employed in several nations outside of Europe, with some early success. Adapting acceptable practices in-line with European values is a challenge that needs to be met. Based on a review of country cases, existing technologies, and European legislation, the following recommendations are made for Austrian, Dutch, and European Union governmental stakeholders alike to apply, as appropriate, within a whole of government, whole of nation, and whole of union framework.

1. **Consider, where not already adequately provisioned for in existing law, new legal provisions to better be able to use data and ICT to combat the present coronavirus pandemic.** All measures should be drafted in a multistakeholder environment, should be time-limited for the length of the emergency (sunset provisions), and support both privacy-by-design as well as post-hoc privacy audits to evaluate both "justified use" as well as discover any irregularities or misuse of the provisions.
2. **Support the deployment of voluntary, user-controlled self-identification mobile phone apps** based on the reviewed case of "TraceTogether" (Singapore) and "StoppCorona" (Austrian Red Cross). The principle should be user self-identification and authoritative verification of positive testing.
3. **Continue the use of anonymized mobile network telecommunications data to evaluate general trends in the epidemiological spread and general population movements (i.e. "heat maps")**. Examples include the provision of data to relevant authorities by the Austrian A1 and the German Telekom[2], and the EU Commission's call to telecom giants for greater access to anonymized data for purposes of epidemiological tracking.

[1] UN News: *COVID-19: UN chief calls for global ceasefire to focus on 'the true fight of our lives'*: https://news.un.org/en/story/2020/03/1059972.
[2] Pollina, Elvira & Busvine, Douglas: *"European mobile operators share data for coronavirus fight"*, Reuters: https://www.scmp.com/tech/policy/article/3075871/european-mobile-operators-share-location-data-coronavirus-fight-italy Der Standard: *"Ist das Handy-Tracking von A1 vertretbar?"*, https://www.derstandard.at/story/2000116136360/ist-das-handy-tracking-a1-vertretbar.

4. **Evaluate digital procedures to support self- and legally mandated quarantines**. These should consider the South Korean and Taiwan models in particular. The existence of a Polish quarantine app should be noted.
5. **Prepare European measures to allow for inner-Schengen movement and international travel in and out of the Schengen zone.** The EU is to examine the possibility of using the Schengen Information System II to enable better registration and contact tracing of international travelers. The examples of South Korea and Taiwan should be considered.
6. **Explore new big data management provisions at European level that, in consideration of existing legislation** (GDPR, ePrivacy directive, etc.) better support the development of artificial intelligence and big data solutions to combat the coronavirus pandemic.
7. **Consider, at all levels of government, new forms of multistakeholder consultation that will explore all relevant data and ICT aspects.** The "Digital Pandemic Agenda" should include and go beyond immediate epidemiological requirements and should address "secondary" concerns including in Internet communication infrastructure deployment, education, data protection, economic activities, and more.

Overall, this report encourages all stakeholders to consider **a principle of "data for the common good".** While the EU Commission has already framed a specific and noteworthy program using this term[3], all stakeholders are recommended to look further, and consider adopting the concept as a general principle. For the current coronavirus pandemic has shown that our basic approach to data should be reconsidered. The reconciliation between the needs of Internet business giants and business in general, the secret practices of government national security organizations, the efforts of rights advocates and lawmakers to protect citizens and national interests, and the desire for all those involved to be able to engage in unrestricted research and innovation needs to be rethought. The easiest way to start the discussion is to reconsider where an overriding common good interest can be applied to both private as well as government data collection activities, and where there is an overriding personal interest. But most importantly, our citizens need to be better educated as to the data reality that we now inhabit, its dangers and promises, so that they can be better empowered to make their own decisions on how the data they generate is used. While the coronavirus pandemic represents a clear and present danger to our individual and collective welfare, it is also an opportunity for Europe to rethink its relationship with data overall – and where we want it to take us.

[3] Stolton, Samuel: *"Commission touts importance of 'data for common good' amid COVID-19 privacy concerns"*, EURACTIV: https://www.euractiv.com/section/digital/news/commission-touts-importance-of-data-for-common-good-amid-covid-19-privacy-concerns/.

Table of Contents

2. Analysis: Overcoming Cyber Cognitive Dissonance

2.1. COVID-19, Information Technology, and Cognitive Dissonance

"The real danger is the (cognitive) dissonance this virus creates"

~ Yves Daccord, Director-General of the ICRC[4]

Cognitive dissonance is a discomfort caused by holding conflicting elements of knowledge. It is often summarized as the tendency of humans to effectively create their own realities when faced with information that contradicts their own imminent beliefs or goes against their own perceived self-interest. While cognitive dissonance can arise in any context of modern life, a Harvard psychologist described it as particularly acute when humans are confronted with a new scientific theory.[5]

The current global coronavirus pandemic presents several unique challenges to humanity – local and national crisis management measures and individual efforts versus international cooperation and joint efforts, globalized supply chains and international travel versus the needs of large-scale containment, and in general the efficiency versus resiliency of many of our systems of daily life. One of the most significant challenges of the pandemic is however conceptual: the high transmission rate of the SARS-CoV2 virus,[6] the fact that the carrier is infectious for days before any symptoms are shown,[7] the often mild symptoms outside of vulnerable populations, and the overall relatively low mortality rates[8] have often posed a cognitive challenge not only for the population at large, but sometimes for educated observers and public leaders. Even educated professionals are easily misled to make comparisons with the influenza virus, which for many nations poses the most significant yearly public health challenge[9], underestimating both the direct threat of the virus itself as well as the secondary effects of severely strained or even collapsed public health systems. On a call with Harvard University on March 19, 2020, the Director-General of the International Committee of the Red Cross (ICRC) Yves Daccord put it as: "The great danger of the present situation is the (cognitive) dissonance the virus creates – between the personal risk, which is very low, and the community risk, which is very high."[10] The implication is that when faced with this dissonance, it is unfortunately natural to ignore or side-line the community risk. A similar related effect is equally visible amongst "science-hostile" segments of the voting population in the United States and elsewhere, amongst whom the political statement "the people are sick of experts" rings true for purely ideological reasons.

The coronavirus pandemic, however, not only causes cognitive dissonance through its own particularities, but also accentuates existing dissonances. One particularly relevant dissonance is the functioning and working of modern Internet-enabled features of daily life – like social media, Internet search functions, and

4 Derived from personal transcript of the Harvard University - International Committee of the Red Cross (ICRC) Call March 19, 2020.
5 *Perlovsky, Leonid: "A Challenge to Human Evolution – Cognitive Dissonance", Frontiers in Psychology:* https://www.frontiersin.org/articles/10.3389/fpsyg.2013.00179/full; https://www.frontiersin.org/articles/10.3389/fpsyg.2013.00179/full
6 Basic reproduction numbers of SARS CoV2 (in effect the basic transmission rate) are set at 2.5 versus 1.5 for the so-called seasonal flu. Callaway, Ewen et. al.: "*The coronavirus pandemic in five powerful charts"*, Nature: https://www.nature.com/articles/d41586-020-00758-2.
7 *Coronavirus Resource Center: "As Coronavirus Spreads, Many Questions and Some Answers", Harvard Medical School:* https://www.health.harvard.edu/diseases-and-conditions/coronavirus-resource-center
8 *Abadi, Mark; Cooper, Havovi & Teckman-Fullard, Meg: "How the Coronavirus Compares to SARS, Swine Flu, Zika and Other Epidemics",* https://www.businessinsider.com/coronavirus-compared-to-sars-swine-flu-mers-zika-2020-3?r=US&IR=T
9 *World Health Organization: "SDR, Influenza, per 100,000", European Health Information Gateway:* https://gateway.euro.who.int/en/indicators/hfamdb_415-sdr-influenza-per-100-000/
10 Derived from personal transcript of the Harvard University -ICRC Call March 19, 2020.

even basic traffic routing – and the deployment by governments of what is commonly described as "surveillance technology". On the most basic level, most users are aware that to enable virtually any basic Internet-based services, they engage in a trade – providing "personal data" in exchange for an otherwise fee-free service, like using Google or Facebook. This personal data includes search or contact preferences, viewing behavior, access times and technologies (like browsers and PCs), and location data – the relevance of the latter having increased markedly in recent years. While most users are aware that their providers directly monetize this information via various marketing strategies, this data is also directly needed to help provide the service to begin with. This "operationally relevant" data includes often enough most of the same information that is sold or used directly for marketing, and this also includes the particularly important "location data" – often a combination of Internet Protocol numbers and GPS or assisted GPS (A-GPS) data when used by mobile phones. Together, this can give commercial services remarkable transparency as to what is occurring within a specific area.

Google's search data alone, for instance, has repeatedly been able to show the spread of a disease in real-time, hours or day before the information was reported to the US Center for Disease Control (CDC). Additionally, it can predict when and where an outbreak is likely to occur, possibly before it actually happens.[11] Web search queries were one of the first digital sources used for the analysis of disease trends, and Google Flu Trends, one of the earliest applications, initially claimed it could track trends one-two weeks faster than the CDC, but was dropped in 2015 after its estimates proved inaccurate by 140%.[12] While Google Flu Trends might have failed, the company made flu-related search data available to the CDC as well as researchers to improve the methodology. Similar initiatives that aim to share data for the public good while respecting privacy have followed suit, but most of these remain relatively small and fragmented efforts.

This type of clairvoyance is not limited to Google. Digital epidemiological tracking methods that have been used to track the flu or other disease trends and movements in near real-time also include sources from social media platforms, news rooms, blogs, and online news media,[13] as well as flight information.[14] Small companies using their own special datasets – often built on special relationships with large data aggregators like Facebook – can also deliver the breakthrough analysis. For instance, the current coronavirus pandemic was predicted by a small artificial intelligence company called BlueDot, which issued its own warnings in December 30, 2019 - beating the US Center for Disease Control (CDC) and World Health Organization (WHO) by a nearly 10 days. It also correctly predicted the spread of the virus to Tokyo, and beyond.[15] These kind of methods can serve as an early warning system that provides local and timely details

[11] *IANS: "Tool That Uses Google Search Data to Track Dengue", Economic Times:* https://economictimes.indiatimes.com/news/science/tool-that-uses-google-search-data-to-track-dengue/articleshow/59698697.cms?from=mdr.
[12] Lazer, David & Kennedy, Ryan: *"What we can Learn from the Epic Failure of Google Flu Trends"*, WIRED: https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/.
[13] As seen in Haiti and the H1N1 outbreak, Twitter was able to accurately track reported disease levels in real time and perform sentiment analysis related to the outbreak. Bates, Mary: "*Tracking Disease: Digital Epidemiology Offers New Promise in Predicting Outbreaks"* IEEE Pulse: https://pulse.embs.org/january-2017/tracking-disease/.
[14] Access to global airline ticketing data can help predict where and when those infected with a virus are traveling to next. By applying machine learning to flight data, BlueDot predicted that COVID19 would go from Wuhan to Bangkok, Seoul, Taipei and Tokyo immediately after. *Niiler, Eric: "An AI Epidemiologist Sent the First Warnings of the Wuhan Virus", WIRED:* https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/.
[15] *Ibid.*

about disease outbreaks and related events on a global scale, thereby decreasing the time between an outbreak and formal recognition of an outbreak, allowing for expedited response.[16]

At the same time many users seem to be opposed to the rationale that their own governments get the same – or even some – of the same data. This is not only true for personal data like Internet search histories and the like, but also for location data, and even general metadata – like whom called whom and for how long (rather than the contents of the call). This dissonance in user preferences seems particular to liberal democracies (a number of studies have shown in different populations a fairly cavalier attitude to government collection of some metadata)[17] which has never been adequately accounted for but is often explained with a combination of historic lack of trust in government plus the realization that governments can actually impose sanctions for real or perceived misbehavior. Google, after all, is not going to put someone in jail or issue a tax audit based on their search history.

In contrast, telecom providers – the backbone of both mobile (incl. smartphone) and fixed-line (e.g. domestic home use) Internet services – will have less traffic data, usually limited to connection metadata (i.e. showing a connection to Google rather than what is being searched for, or the time and length and number of a phone call rather than the content of a phone call), and most relevantly the location data provided via their own mobile phone base station networks.

How accurate is a telecom provider's location data? Unlike what has recently been reported in European media, the specifics can vary greatly. Using the most basic triangulation methods all providers can achieve accuracies of around 100m in areas with high antenna densities, with up to 50m accuracy under specific conditions and using more advanced methods – however in areas with low density (for instance rural areas without many antennas) accuracies can be a kilometer or more. But some providers may be able to used more advanced techniques (like RRLP), or are capable of exploiting the SS7 baseband GSM protocol system, which provides direct access to the mobile phone's own much more accurate GPS data – and in both cases accuracy of 10m can be achieved. Therefore, the only universally honest answer is "it depends" – some countries and their telecom providers are certainly able to achieve highly accurate locations with their national security surveillance apparatus. And these national security structures are not commonly in the public eye and their capacities are seldom if ever reported on.

2.2. COVID-19 Contact Tracing & Quarantine (CTQ) Necessities

As of March 25, 2020, the John Hopkins Corona dashboard indicated 466,000 confirmed cases of COVID-19, affecting 196 countries and territories.[18] The virus has a higher transmission rate than either the 2003 SARS or the 2008 MEV outbreaks. Mortality rates have doubled nearly every three days in cases like Spain,

[16] Salathé M, Bengtsson L, Bodnar TJ, Brewer DD, Brownstein JS, Buckee C, et al.: "*Digital Epidemiology*". PLoS Comput Biol 8(7): e1002616. https://doi.org/10.1371/journal.pcbi.1002616

[17] *Fuhrman, Peter: "Government Cyber-Surveillance is the Norm in China – and it's Popular", Washington Post:* https://www.washingtonpost.com/opinions/cyber-surveillance-is-a-way-of-life-in-china/2016/01/29/e4e856dc-c476-11e5-a4aa-f25866ba0dc6_story.html; *Bakir, Vian; Cable, Jonathan; Dencik, Lina; Hintz, Arne; McStay, Andrew: "Public Feeling on Privacy, Security and Surveillance – A Report by DATA-PSST and DCSS", Bangor University; Cardiff University:* https://orca.cf.ac.uk/87335/1/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf.

[18] The John Hopkins Coronavirus Resource Center has an interactive web-based map to track cases of the virus around the world, available at https://coronavirus.jhu.edu/map.html.

the United Kingdom, and the United States.[19] One of the most modest estimates for the US indicated that it would need 200,000 intensive care units in total, although only 40,000 were available, with a fraction of that available during the current influenza epidemic.[20] Estimates of the duration of the pandemic range from months to years and are contingent upon many variables such as the seasonality of the virus, the possibility of reinfection, mutation rate, and preventative measures. With the virus becoming endemic in Europe and much of the world, it is possible that, like the influenza virus, it may return annually. The media reports of expert estimations of a general vaccination becoming widely available range from December 2020 and continues until Fall of 2021.[21]

The most commonly assigned protective strategy to deal with the infection is contact tracing of carriers and rapid physical quarantine (CTQ) to prevent transmission. Both Singapore and Taiwan[22] have won praise for their approach to CTQ in rapidly identifying possibly exposed individuals by making use of a variety of applications. This has been credited with vastly shortening the window within which infected individuals could spread the COVID-19 virus. Using contact tracing, a positive COVID-19 test immediately yielded a list of other high-risk individuals who could then be tested.[23] In addition, South Korea has won praise for its public disclosures of infection hotspots[24]. By making use of CTQ tools it could push out regional notifications[25] on which areas should be avoided. All three cases have made extensive use of location monitoring to more effectively enforce quarantines.[26] This includes GPS tracking and automated notifications to law enforcement officials if a quarantined individual was found outside the quarantine zone.

2.3. Summary of Country Case Studies Approaches

Several counties were selected as CTQ case studies detailed in Appendix A: Taiwan, South Korea, Singapore, China, and Israel. While most are to be considered democracies and "free societies" (using the Freedom House Index), there are also more authoritarian models included as well.[27] This is justified on the basis that all the countries in question took relatively early measures to deal with the coronavirus pandemic and showed strong results, and it is interesting to see how the relatively "free" or "less free" societies have approached the issue with similar programs.

[19] Katz, Josh and Sanger-Katz, Margot, "*Coronavirus Deaths by U.S. State and Country Over Time: Daily Tracking",* The New York Times: https://www.nytimes.com/interactive/2020/03/21/upshot/coronavirus-deaths-by-country.html.
[20] ICRC CEO Yves Daccord, Harvard, ICRC Call March 19, 2020.
[21] Shapiro, Marc:New *Coronavirus Vaccine in Development at Johns Hopkins", Johns Hopkins Medicine:* https://www.hopkinsmedicine.org/coronavirus/vaccine-development.html*;* Wood, Graeme and Spiegel, David A.: *"COVID-19 Vaccines Are Coming, but They're Not What You Think - These novel approaches could fail in many ways.", The Atlantic: https://www.theatlantic.com/ideas/archive/2020/03/two-extreme-long-shots-could-save-us-coronavirus/608539/.*
[22] Shapiro, Don: "*Taiwan shows its mettle in coronavirus crisis, while the WHO is MIA"*, Brookings Institute: https://www.brookings.edu/blog/order-from-chaos/2020/03/19/taiwan-shows-its-mettle-in-coronavirus-crisis-while-the-who-is-mia/.
[23] Baharudin, Hariz: "Coronavirus: S'pore Government to make its contact-tracing app freely available to developers worldwide", The Strait Times: https://www.straitstimes.com/singapore/coronavirus-spore-government-to-make-its-contact-tracing-app-freely-available-to.
[24] Yoon, Dasl and Martin, Timothy W.: "Why a South Korean Church Was the Perfect Petri Dish for Coronavirus", The Wall Street Journal: https://www.wsj.com/articles/why-a-south-korean-church-was-the-perfect-petri-dish-for-coronavirus-11583082110.
[25] Kim, Max S.: "South Korea is watching quarantined citizens with a smartphone app", MIT Technology Review: https://www.technologyreview.com/s/615329/coronavirus-south-korea-smartphone-app-quarantine/.
[26] Yong, Clement: "How quarantine orders, stay-home notices differ", The Strait Times: https://www.straitstimes.com/singapore/how-quarantine-orders-stay-home-notices-differ.
[27] Freedom House Index considered the following societies as "free" (with relative score): Taiwan (93), South Korea (83), Israel (76); "semi-free": Singapore (50); "not free": China (10). Derived from: https://freedomhouse.org/explore-the-map?type=fiw&year=2020.

Overall, this report distinguishes "user-based" and "provider-based" CTQ measures. User-based measures are those that the individual user has direct control over, and ranges from purely voluntary measures like the Singaporean "Let's Track" crowdsourced app which uses QR codes to voluntary register personal movement to the semi-compulsory "quarantine phone" provided by the Taiwanese and Singaporean governments. The "provider-based" measures are those that are largely executed by the telecom backbone providers. These range from highly anonymized measures (for instance A1 Telekom Austria Group sharing results from a motion analysis application by contractor Invenium)[28] to highly targeted measures (including individually identified cell phone location and tracking).

Within the national case studies, two conclusions are apparent:

1. The public **emphasis is on user-based approaches**, including both those of primarily voluntary nature as well as those with some level of compulsion. However, provider-based measures seem to be omnipresent
2. The more democratic nations **openly discuss provider-based CTQ surveillance architectures**, while less democratic nations do not or hide them completely.

2.3.1. Provider-based CTQ measures

The reviewed provider-based (i.e. telecom operators) CTQ measures can roughly be divided into three categories[29]:

1. **Information and awareness purposes:** Using (pseudo)anonymized data stripped of identifiers which can help show adherence to quarantine procedures by mapping the amount of anonymized movement in a particular area. This does not require exact locations or identities to be known. These can be fully formalized apps including the "Corona 100m" app used in South Korea, the "Tencent Corona Tracking Map" used in China.[30] Mostly invisible to the public is anonymous data analyzed by, for example, the Austrian, German and Italian telecom operators[31] to provide information on general quarantine adherence practices, which only counted "numbers of cell phone users in motion" rather than a specific identifier.
2. **Quarantine Enforcement:** Using basic cell station triangulation techniques individuals can be "geofenced" to a specific area, like their place of residence. While maximum accuracy of the exact location is still limited to around 100m (using U-TDOA technique) or 30m (using E-OTD) in optimal conditions, this is sufficient to map the immediate vicinity of the quarantined individual. However, vertical movement (for instance multistory buildings) will largely be invisible to this system. Examples of this technique include the Taiwanese quarantine procedures.[32]
3. **Contact Tracing and Cross-Referencing:** To be useful for contact tracing the best case 50-100m radius of normal triangulation techniques will not be sufficient. Instead, advanced localization

[28] Pollina Elvira & Busvine, Douglas: *"European mobile operators share data for coronavirus fight"*, Reuters: https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2
[29] See Appendix B on basic geolocation tracking
[30] See Appendix A case studies
[31] *Pollina, Elvira; Busvine, Douglas: "European Mobile Operators Share Data for Coronavirus Fight", Reuters:* https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2
[32] See Appendix A case study

techniques (for instance using RRLP[33]) or even "baseband exploitation" needs to be used. Baseband exploitation commonly refers to attacking the known weakness of the basic GSM SS7 protocol that are impossible to patch, and which effectively can give an attacker total access over any GSM enabled device.[34] In this case, the attacker can also access the A-GPS data generated by the phone itself and which normally the telecom provider does not have access to, and results in accuracy of up to 5m. When this specific location data is cross-referenced with known health data of other individuals (possible COVID-19 carriers) and used with time-measurement records (the length of time the individuals are in proximity with each other) likely estimates on chances of infection can be deduced. Currently the only publicly known example of this technique is the Israeli internal security system detailed in the Appendix A, but other literature shows that both Singapore and especially China may very well have this capability as well.[35]

2.3.2. User-based CTQ measures

The review identified a number of user-based CTQ measures, meaning that the individual provides the data upwards, most likely via their mobile phone, rather than being covertly tracked by a telecom provider. However, at higher levels there is a merging of the two approaches. A basic three-part categorization is made:

1. **Voluntary provision and crowdsourcing of infection data:** A number of apps have been developed that allow the user to participate in a crowd-sourced reporting of infections. One of the earliest and most successful is the Singapore's "Let's Track App", the source code of which is provided for free by the Singaporean government. This app and others like it often work along the same premise: the user is asked to activate their Bluetooth feature on their phone at all times. If they test positive for COVID-19 they (or ideally, a licensed healthcare professional) report this via their app, which then uses the precise movement history of the phone to check with other app users registered via Bluetooth within the virus' transmission window. These individuals are then directly notified via SMS or email. Austria's Red Cross uses the "Stopp Corona" app as a "digital contact diary" that enables users to keep an anonymized digital log of the people they meet at what time.[36] If a person falls ill with COVID-19, these contact persons can be notified. The "digital handshake" is not automatic and needs to be confirmed by the user. Another example of voluntary provision of data seems much more intrusive – this being the voluntary provision of a patient's phone to enable the extraction of visited locations in order to support the contact tracing. This feature is also used in Singapore, using technology from an Israeli company, on a voluntary basis.[37]
2. **Quarantine Monitoring by app.** Some countries are using apps to support quarantine procedures that would have to be supervised by daily physical visits or provider-based data. Taiwan, South Korea and Poland[38] have developed apps that report the location of the phone as well as requests for "selfies"

[33] *European Patent Office: "Delayed Radio Resource Signalling in a Mobile Radio Network", Google Patents:* https://patents.google.com/patent/EP2212710B1/en
[34] See for instance*: "IT Report: A Phone Number is Sufficient to Hit a Person With a Drone Missile", Netzpolitik:* https://netzpolitik.org/2016/informatik-gutachten-eine-telefonnummer-ist-ausreichend-um-eine-person-mit-einer-drohnen-rakete-zu-treffen/
[35] The basic assumption of baseband exploitation is a common reason why European governments advise their civil servants to not take their personal devices to China.
[36] *Austrian Red Cross: "Stopp Corona – Mein Kontakt-Tagebuch": https://www.roteskreuz.at/site/faq-app-stopp-corona/*
[37] Interview
[38] Poland launched a "home quarantine" app that uses geolocation and facial recognition to allow people under quarantine for the coronavirus to send selfies to the authorities to confirm they remain home. The police is notified if the user does not respond to the

of the patient to confirm they are adhering to quarantine procedures and haven't simply left the phone at home. For "special cases" (including those without smartphones) Taiwan and Singapore have taken to providing government-issued phones directly.

3. **QR code provided registration tracking:** Using QR codes to self-register at locations – described as filling out forms digitally – can range from being the "supplementary" to the "encompassing". Singapore uses QR codes primarily as a "form filling" device – individuals are required to sign in to specific public locations that they visit using the QR codes, sometimes voluntarily, but sometimes it is mandatory.[39] This is supposed to support later contact tracing measures if needed – should the individual need to be contacted it is done by phone directly. China has gone further: the QR code system is not only a passive sign-in device but also directly a public ID of one's allowed movement level, color-coded by green, yellow, or red. This is particularly important to supplement the pervasive physical checks that accompanied the Chinese lockdown. Post lock-down China is moving towards a system which apply a similar color-coded approach to schools and universities.

2.4. Data Protection, National Security Means, and COVID-19 CTQ

The Asian CTQ case studies summarized above and reviewed in detail in Appendix A all have one thing in common: their governments engaged in-depth pandemic preparedness planning following the 2003 SARS epidemic. The lessons learned from this pubic heath disaster were directly integrated into emergency plans that included the measures described above. Despite a Eurocentric tendency to claim the contrary, data protection concerns are not unknown in the case studies reviewed above – especially in Taiwan and South Korea, both ranked highly by Freedom House as liberal democracies. These countries have not only made their own equity analysis as to the expected risks to civic rights and benefits to public health, but have done something more – a transparent and full accounting of what commercial and governmental (national security) technology is constantly engaging in.

In the case studies it was revealing to what extent the democracies openly talked about employing national security means in a CTQ context. While this report does not recommend the adoption of the provider-based (telecom operator-based) individual CTQ tracking within a European context unless under further emergency provisions, both the revealed national capabilities of the case studies in question as well as the overall discussion on the use of data are instructive – namely who is willing to talk about capabilities, and who is not.

It is interesting to note how often Singapore's public communication emphasizes that, when police investigation of a contact case is necessary, this is purely done by the law enforcement officers "reviewing CCTV footage and asking the right questions".[40] Singapore is largely considered to be one of the most heavily digitally surveilled societies. Although details of the domestic surveillance apparatus are not

request in 20 minutes. "People in quarantine have a choice: either receive unexpected visits from the police, or download this app," Karol Manys, digital ministry spokesman, told AFP. AFP: "'Selfie app' to keep track of quarantined Poles", France 24: https://www.france24.com/en/20200320-selfie-app-to-keep-track-of-quarantined-poles.

[39] *Min, Ang Hwee: "NTU to Log Student Attendance via QR Codes to Facilitate Contact Tracing for Coronavirus Outbreak if Needed", Channel News Asia:* https://www.channelnewsasia.com/news/singapore/wuhan-virus-ntu-contact-tracing-attendance-qr-codes-12422134

[40] Mahmud, Aqil Hazig: *"'Like an invisible criminal': How police helped find missing link between COVID-19 church clusters in a day",* Channel News Asia: https://www.channelnewsasia.com/news/singapore/police-missing-link-church-clusters-covid19-coronavirus-12509492.

known, in 2015 a Privacy International report stated that "it is widely acknowledged that Singapore has a well-established, centrally controlled technological surveillance system designed to maintain social order and protect national interest and national security [...] The surveillance structure in Singapore spreads wide from CCTV, drones, Internet monitoring, access to communications data, mandatory SIM card registration, identification required for registration to certain website, the use of big data analytics for governance initiatives including traffic monitoring."[41] It is virtually unthinkable that this infrastructure – especially the comparatively easy location-tracking of individual cellphone users – is not employed in a CTQ context. However no information is made available, and in pubic communication Singapore puts great stock in the "self-reporting" of individuals, using for instance their QR codes.[42] China is an even more extreme surveillance example, as noted in the relevant case study, and unlike Singapore has no claims of being a democracy. China has sometimes even boasted about its internal surveillance capabilities – for instance, reports on the extensive surveillance infrastructure deployed in the province of Xinjiang are easily confirmed by official sources and state contractors, who often enough are happy to show their capabilities in what is widely considered to be show of power.[43] However, Chinese authorities have been extremely reluctant to show how these same capabilities have been used in the current pandemic crisis.

Data protection has precise aims to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors. Within the European Union, privacy is equated with a right to private life and with dignity. It is therefore a fundamental value. It connects directly to the Universal Declaration of Human Rights (Article 12). In Europe, the notion of data protection originates from this right to privacy and is instrumental in preserving and promoting fundamental values and rights as well as the ability to exercise other rights and freedoms – such as free speech or the right to assembly.[44] While some human rights are considered "absolute" and apply in all cases, most have legitimate limitations that can be applied under special circumstances. For instance, in most European Member States currently the right to movement and right to assembly has been greatly curtailed. A similar momentarily curtailment of the right to privacy is also legally possible.

However, currently some of the more extreme data protection voices have questioned the use of even anonymized provider data. For instance, the Austrian and German telecom providers have taken to delivering highly generalized "heat maps"[45] of population movements to provide feedback on quarantine measures. Although clearly legal even without emergency provisions, some of the data protection voices have either made blanket statements on how useless these measures would be for epidemiological purposes (although the actual medical experts in the field say the opposite) or spread technical incorrect information, for instance on what accuracy is possible for the providers. Although the former is a

41 Privacy International: "*The Right to Privacy in Singapore*": https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf.
42 The Singapore QR code-based tracking is likely useful, but how useful depends on the exact provider-based surveillance capabilities deployed in the background. If the abilities of national provider Singtel are akin to most European telecom providers, then the accuracy will be much too low to be useful for CTQ measures especially in a multi-stored urban area. If, however, the location accuracies are more akin to what Israel or China are presumed to be able to deliver then QR code usefulness would be largely psychological.
43 Buckley, Chris & Mozur, Paul: *"How China Uses High-Tech Surveillance to Subdue Minorities",* The New York Times: https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.
44 See for instance: https://edps.europa.eu/data-protection/data-protection_en
45 Pollina, Elvira & Busvine, Douglas: *"European mobile operators share data for coronavirus fight",* Reuters: https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2, Der Standard: *"Ist das Handy-Tracking von A1 vertretbar?",* https://www.derstandard.at/story/2000116136360/ist-das-handy-tracking-a1-vertretbar.

transparent moral failing, the latter is particularly dangerous: by spreading incorrect information, it makes it less likely that national security means, even in Europe, will be discussed as openly as they have been elsewhere.

The ideological nature of the debate – away from the actual capabilities of some governments, even in Europe – means that the discussion is not taking place with the level of openness that the crisis requires. This has spillover effects on how general CTQ measures are considered even within the EU. Two recent examples show how far from each other the approaches can be. The Austrian Red Cross is promoting the "Stopp Corona" app[46] as a "digital contact diary" that enables a user to keep an anonymized digital log of the people they meet at what time. If a person falls ill with COVID-19, these contact persons can be notified. The "digital handshake" is not automatic and needs to be confirmed by the user. The data is completely resident with the users and the use is voluntary.[47] Virtually opposite to that, Poland recently launched a "home quarantine" app that uses geolocation and facial recognition to allow people under quarantine for the coronavirus to send selfies to the authorities to confirm they remain home. The police are notified if the user does not respond to the request in 20 minutes. "People in quarantine have a choice: either receive unexpected visits from the police, or download this app," Karol Manys, digital ministry spokesman, told AFP.[48]

Ultimately, some data protection researchers have made it clear that there may well be grounds for temporarily superseding some of the privacy rights – as long as these suspensions are temporary.[49] This, effectively, is the crux. The current coronavirus pandemic emergency is exactly that – an emergency that most EU Member States are approaching without the in-depth planning the Asian case studies undertook after the 2003 SARS epidemic. The majority opinion among the epidemiological experts is that developing and deploying a vaccine would take at least until December 2020, and possibly extend to the fall of 2021 – with new infection peaks possible in the meantime. Therefore, the emergency measures need to be considered for the entire duration of the expected emergency – not only the present crisis.

2.5. Comments on the Recommendations

This report has only recommended technical CTQ measures (see recommendations) that are clearly within existing EU legislation. However, new legal provisions may become necessary at European or Member States level. Three principles are proposed here to ensure best compliance with EU values:

- ***Multistakeholder consultation****:* besides the regular legislative processes and work of lawmakers, it is recommended that all potential measures be considered in bespoke "whole of nation" or "whole of union" configurations, with state and non-state actors and experts present, according to specific needs. This should include data protection advocates as well as academic experts and professionals from

[46] Bürger, Jasmin: *"Stop Corona: App should slow down spreading"*, World Today News: https://world-today-news.com/stop-corona-app-should-slow-down-spreading/.
[47] https://www.roteskreuz.at/site/faq-app-stopp-corona/
[48] AFP: "'Selfie app' to keep track of quarantined Poles", France 24: https://www.france24.com/en/20200320-selfie-app-to-keep-track-of-quarantined-poles.
[49] Sulzbacher, Markus & Al-Youssef, Muzayen: *"Mobilfunker A1 liefert Bewegungsströme von Handynutzern an Regierung"*, Der Standard: https://www.derstandard.at/story/2000115828957/mobilfunker-a1-liefert-bewegungsstroeme-von-handynutzern-der-regierung.

industry as well as military, law enforcement and intelligence. Their remit should not be to question the medical and epidemiological advice, but to provide solutions to the scenarios that they create.

- ***Time limitation of measures**:* whatever exceptional measures are taken must be defined as such, with a clear automatic termination period (sunset clause) or other limitation of duration.
- ***Post-hoc auditability:*** to strengthen the trust in the proportionality of the measures employed, special consideration should be given to creating a clearly investigable audit trail to consider the "justified use" of the data after the emergency has passed and the provisions have lapsed. This can be facilitated by privacy-by-design methods in designing and deploying the technical tools themselves.

Further, from a EU perspective special consideration must be given on how to manage the resumption of free movement of people and goods as soon as possible. Under the immediate "crisis" situation it is difficult to envision a resumption of the free movement of people in Europe, however, in the continuing "emergency" situation it will be necessary to restart the inner-European movements as well as international travel. For the latter, a challenge will be to prevent reinfection from hotspots outside of Europe – for instance from South or North America. It is advisable to therefore consider harmonizing border procedures and expanding the options of the Schengen Information System II (SIS2) to adequately allow for travelers from outside of the EU to be properly registered and, if necessary, contacted – similar to how Taiwan has operated.

Slightly out of scope of the present study but crucial for CTQ measures is some form of European initiative to better mobilize European big data and ICT resources to help support all kinds of pandemic crisis mitigation efforts. A constant and at least somewhat justified lament is that European legislation has been a major stumbling block in creating new data-driven services, particularly in the field of artificial intelligence and big data analytics. Commiserate to the existing emergency, the EU institutions should take the lead in examining, as one EU program proclaims, what exactly "data for the common good" entails.[50] Optimally the "data for the common good" should be seen as being more than a project-line title, and instead be reconceived of as a "principle". This principle can help refocus the discussion on data in Europe, which itself suffers from a case of cognitive dissonance: while significant effort has been expended on data protection and privacy measures, some Member States' own digital surveillance measures are very advanced. At the same time, some governments have created deep covert capabilities, and foreign (outside EU) companies can hold more personal identifiable information on EU citizens then their own governments likely do outside the security services.

Finally, the current crisis also has shown some significant latent European strengths, most apparently in Austria and in the Netherlands – namely the ability of actors outside the normal channels of government to productively and proactively support government emergency measures. In the field of ICT, in particular Internet governance, the governance model is often entitled "multistakeholder engagement". While multistakeholder engagement can mean different things in different circumstances, it fundamentally involves the structured engagement of all relevant state and non-state actors in policy discussions. The need is particularly acute where the topics are complex and have multiple interdependencies, where no single actor is likely to have an encompassing answer – as is the case within the "digital" realm. The number

[50] Stolton, Samuel: "*Digital Brief: Data for the Common Good?*", EURACTIV: https://www.euractiv.com/section/digital/news/digital-brief-data-for-the-common-good/.

of “digital” issues relevant to the pandemic are considerable and could be encapsulated in a “Digital Agenda for Pandemic Response”. This could include discussions on CTQ measures but go beyond that, to discuss issues of basic telecom infrastructure (including bandwidth provision), education (home schooling support), economy (supply chain, delivery and home office), and much more. Optimally, every EU Member State government would have such a strong advisory and consultation structure on a national level, potentially attached to the head of government function, and it would be mirrored by similar policy groups within the EU institutions. For although the length, duration and ultimate human and economic impact of the current coronavirus pandemic are unknown, ultimately it will be a question of good governance – rather than good technology – that will decide if this is a fight that will make Europe and liberal democracies stronger – or if it will tear them apart.

Appendix A: Country Case Studies

The purpose of this brief is to provide a conceptual framework and best practices for the application of technology to manage the corona crisis. Efforts to manage the crisis may be broadly categorized into three different buckets:

1. Contact tracing and monitoring of infections
2. Quarantine enforcement measures
3. Public communication

Cases have been drawn from 5 countries[51] running through the following structure:

1. Short summary of country approach
2. Background study on pre-existing surveillance infrastructure
3. Best practices

In addition, an overview of key properties for each country is evaluated on the basis of their approach and data source:

Country	Approach	Data Source
Taiwan	Linking databases and geofencing	Mixed, mostly Provider Based
South Korea	Testing first, geofencing and linking databases	Mixed
Singapore	Public data release, case tracking	Ostensibly mostly User Based
China	Linking databases, enforced compliance, restriction of resources	Mostly Provider based
Israel	Geofencing and linking databases	Purely provider based

Country study 1: Taiwan

The Taiwanese approach is characterized by high transparency on all measures, **including on provider-based tracking, linking of databases, and segmenting of risk categories to streamline processing**. Taiwan has an extensive system of CCTV and is home to numerous CCTV companies[52]. Numerous smart city initiatives exist in Taiwan and extensive use is made of data-driven policy making. Examples include the national health insurance database which includes smart cards that track patient identity and medical history[53]. The widescale use of provider-based cell-phone tracking for enforcing quarantine procedures likely builds on national security capacities.

[51] China, Taiwan, South Korea, Israel, and Singapore
[52] *Chung, Lawrence: "Is Taiwan Becoming a Surveillance State? Privacy Advocates Sound Alarm", South China Morning Post:* https://www.scmp.com/news/china/politics/article/2163365/taiwan-becoming-surveillance-state-privacy-advocates-sound-alarm
[53] *Li, Yu-Chan: "Taiwan HIT Case Study", Health Information Technology and Policy Lab:* https://www.nbr.org/wp-content/uploads/pdfs/programs/TaiwanHIT.pdf

Case 1a: Contact tracing and monitoring of infections[54]

Taiwan has extensive structures put into place in the wake of the 2003 SARS epidemic, including a dedicated outbreak response unit for tracking any anomalous medical situation including anti-biotic resistant tuberculosis[55]. Given the prior experience in the SARS epidemic, the first step Taiwan took was setting up structures for rapid inspections of incoming flights from Wuhan (as early as December 31) and efforts to coordinate the Ministries of Health and Welfare, Transportation, Economics, Labor, Education, and Environmental Protection. The Taiwanese approach has also been **characterized by the merging of datasets,** such as intersecting its National Health Insurance database with its immigrations and customs dataset. The purpose of this was to triage incoming flights for health screening based on recent travel history. This included proactive distribution of health declaration border passes via SMS. Another option was QR codes to report travel and health history for the last 14 days[56]. Subsequent expansions of the dataset lead to 30 days travel history and an expanded set of countries.

Case 1b: Quarantine enforcement measures[57] [58]

14-day quarantine measures are mandatory in Taiwan for all incoming arrivals from high risk regions. In addition, foreign nationals have been banned from entry except under special circumstances. All entrants into Taiwan are required to undertake a 14-day home quarantine or subject to a fine of up to US$ 33.000[59]. All incoming high-risk individuals are given a health declaration and required to electronically sign a quarantine notification form[60]. Face masks are mandatory, as are daily records of body temperatures. **High risk cases are geo-fenced via cellphone tracking and are given a text warning if they are found outside the perimeter**[61]. **The so called "electronic fence" is not voluntary and is not done by app but by the telecom provider** (cell tower triangulation)[62]. If the person under quarantine is seen as moving, they are called. If the cell phone is turned off (for instance due to depleted battery) then the police visit the residence.[63] People with unreliable phone connections or otherwise considered high-risk quarantine were provided government-issued cell phones for the purpose of electronic monitoring; failure to answer official calls leads to heavy fines. Officials call twice a day with activated video calls to ensure people don't avoid tracking by leaving their phones at homes[64].

54 *Duff-Brown, Beth: How Taiwan Used Big Data, Transparency and a Central Command to Protect Its People From Coronavirus, Stanford Health Policy:* https://healthpolicy.fsi.stanford.edu/news/how-taiwan-used-big-data-transparency-central-command-protect-its-people-coronavirus
55 *Taiwan Centers for Disease Control: "Taiwan Epidemiology Bulletin":* https://www.cdc.gov.tw/En/EpidemicTheme/List/dwCswoLnYw874U8oPrVAPA
56 *Moné, Brianna: "Taiwan Has Only 50 Coronavirus Cases. Its Response to the Crisis Shows That Swift Action and Widespread Healthcare can Prevent an Outbreak", Business Insider:* https://www.businessinsider.nl/coronavirus-taiwan-case-study-rapid-response-containment-2020-3?international=true&r=US
57 *Taiwan Centers for Disease Control: "Taiwan Epidemiology Bulletin":* https://www.cdc.gov.tw/En/Category/Page/ONJOb0swWoBKWjZP6ahA3Q
58 *Taiwan Today: "FAQ: Taiwan's 14-Day Quarantine Requirements", Taiwan Today:* https://taiwantoday.tw/news.php?unit=2&post=173589
59 Cole, Brendan: "*Man Fined $33,000 After Breaking Coronavirus Quarantine To Go Partying At Nightclub In Taiwan*", Newsweek: https://www.newsweek.com/taiwan-coronavirus-fine-taipei-quarantine-lockdown-covid-19-1493726.
60 *Ministry of Health and Welfare: "Quarantine System for Entry":* https://hdhq.mohw.gov.tw/
61 *Yun, Michelle: "How Taiwan is Containing Coronavirus – Despite Diplomatic Isolation by China", The Guardian:* https://www.theguardian.com/world/2020/mar/13/how-taiwan-is-containing-coronavirus-despite-diplomatic-isolation-by-china
62 Presumed use of U-DTOA technology. This provides a maximum accuracy of 30m in urban areas but is much less accurate in rural areas, unless specific modifications have been taking. However, the inaccuracy is fixed unless the cell phone power is very weak -– therefore while the "Location" might not be exact the "movement" is discernable.
63 *BBC: "Coronavirus: Under Surveillance and Confined at Home in Taiwan", BBC:* https://www.bbc.com/news/technology-52017993
64 *Lee, Yimou: "Taiwan Tracking Citizen's Phones to Make Sure They Stay Indoors During Coronavirus Lockdown", Independent:* https://www.independent.co.uk/news/world/asia/coronavirus-taiwan-update-phone-tracking-lockdown-quarantine-a9413091.html

For those not in quarantine, face masks are recommended. Production and distribution of surgical masks was quickly nationalized to avoid price gouging and hoarding. Finally, **rationing of masks are achieved through requiring an individual's National Health Insurance card,** and an online ordering mechanism. **Foreigners that lacked such a card had to display their immigration services-provided QR code** for purchasing of masks. Further segmentation took the form of differing procedures for the purchasing of masks based on health status. Furthermore, each region's supply of masks, negative pressure isolation rooms, and other health provisions were mapped.

Case 1c: Public communication[65]

One of the explicit purposes of the Taiwanese approach is to improve information management and create a one-stop information system for quarantine operations along with making the quarantine process and information management more efficient. To that end, a toll-free central hotline was created for citizens to report suspicious symptoms; as full capacity was reached each major city was asked to create its own hotline. The **governments openness in its communication strategy has been credited with maintaining high confidence** in the temporary suspension of privacy rights. Daily media briefings by officials and highly technocratic leadership (Chen Chien-jen, the Taiwanese VP, is a John Hopkins trained epidemiologist)[66] have helped in maintaining high public trust.

Country study 2: South Korea

The South Korean approach is characterized **by high reliance on GPS tracking and widespread testing capabilities, supplemented by provider-based efforts.** South Korea has also seen collaboration between its main telecom companies and law enforcement agencies,[67] and has a long history of domestic surveillance stemming from past military dictatorships. The government has made a distinction between private data and "de-identified data,"[68] where the latter is no longer considered personal data, and can be processed without the consent of data subjects for purposes other than the original intention, such as big data analysis, and can even be provided to third parties[69]. The most recent pieces of data protection legislation passed are the PIPA and ICNA amendments that will take effect in July of 2020[70], the PIPA amendment specifically is aimed at bringing South Korea in line with EU GDPR requirements.

[65] *Waltz, Emily: "Big Data Helps Taiwan Fight Coronavirus", Spectrum:* https://spectrum.ieee.org/the-human-os/biomedical/devices/big-data-helps-taiwan-fight-coronavirus
[66] *Shapiro, Don: "Taiwan Shows Its Mettle in Coronavirus Crisis, While the WHO is MIA", Brookings:* https://www.brookings.edu/blog/order-from-chaos/2020/03/19/taiwan-shows-its-mettle-in-coronavirus-crisis-while-the-who-is-mia/
[67] *Koo, Se-Woong: "South Korea's Invasion of Privacy", New York Times:* https://www.nytimes.com/2015/04/03/opinion/south-koreas-invasion-of-privacy.html
[68] *Lee, Miru: "Data Protection in the Age of Big Data in the Republic of Korea", Global Information Society Watch:* https://giswatch.org/node/6187
[69] *KISA: "Guidelines for Non-Identification of Personal Information",:* https://www.kisa.or.kr/public/laws/laws2_View.jsp?cPage=1&mode=view&p_No=282&b_No=282&d_No=3&ST=T&SV=
[70] *OneTrust Data Guidance: "South Korea- PIPA Amendments: What You Need to Know":* https://www.dataguidance.com/south-korea-pipa-amendments-what-you-need-to-know/

Case 2a: Contact tracing and monitoring of infections[71]

South Korea has made extensive use of GPS tracking and location-based apps. One such volunteer apps is "Corona 100m", which makes use of **provider-based (telecom) data and alerts users if they come within 100 meters of a location visited by an infected person**. Various public website also exist that allow users to keep track of infection hotspots[72]. Furthermore, the South Korean government has created a GPS-enabled app that would set off an alarm if patients in quarantine went outside[73].The availability of data has also created online efforts to identify coronavirus carriers publicly. The South Korean outbreak was highly clustered around the Shincheonji Megachurch in Daegu[74], meaning that

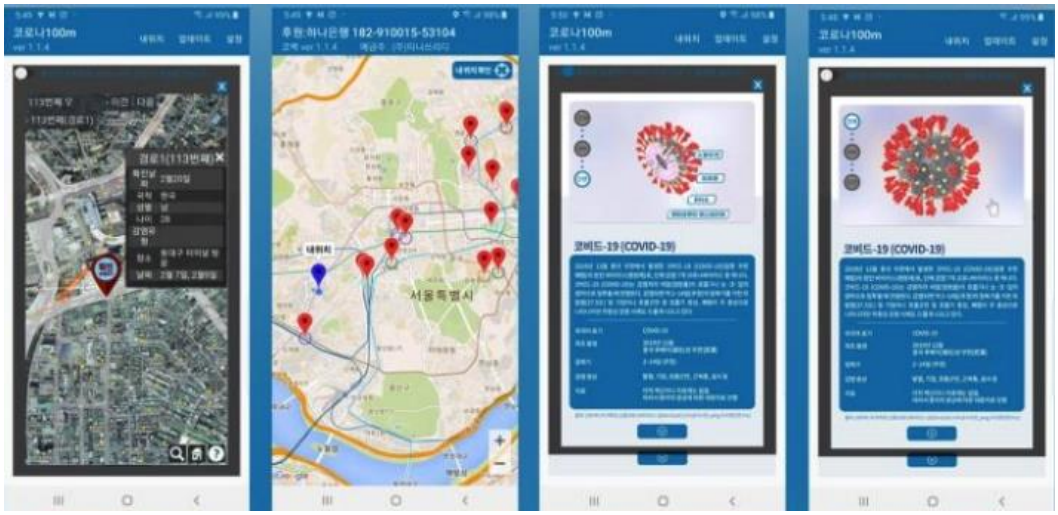

Figure 1 Corona 100m app (*Source: The Guardian*)

contact tracing efforts was focused on that cluster.

Case 2b: Quarantine enforcement measures

Anyone that has encountered a carrier is subject to mandatory quarantine through geo-fencing that is officially monitored via both in-person calls and visits **supplemented by voluntary use of a government provide quarantine app.**[75] Twice daily calls by official and mobile testing teams are implemented as well. The procedure is a patient interview, verification by CCTV footage, credit card records and mobile GPS data[76]. The government then proceeds to release that data via text messages and state-managed websites to allow for hotpot mapping. With the number of people in quarantine reaching 30,000[77], an app was developed to help manage the program. The use of the app is not mandatory and is supplementary to the call monitoring system. In addition to the GPS apps noted above, there have also been efforts made to open

[71] *Wray, Sarah: "South Korea to Step-Up Online Coronavirus Tracking", Smart Cities World:* https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109
[72] *Dong-Hoon, Lee: "Corona Map", CoronaMap:* https://coronamap.site/
[73] *Kim, Max: "South Korea is Watching Quarantined Citizens With a Smartphone App", MIT Technology Review:* https://www.technologyreview.com/s/615329/coronavirus-south-korea-smartphone-app-quarantine/
[74] *Yoon, Dasl & Martin, Timothy: "Why a South Korean Church Was the Perfect Petri Dish for Coronavirus", The Wall Street Journal:* https://www.wsj.com/articles/why-a-south-korean-church-was-the-perfect-petri-dish-for-coronavirus-11583082110
[75] *Kim, Max: "South Korea is Watching Quarantined Citizens With a Smartphone App", MIT Technology Review:* https://www.technologyreview.com/s/615329/coronavirus-south-korea-smartphone-app-quarantine/
[76] *Law, Elizabeth & Choon, Chang May: "How China, South Korea and Taiwan are Using Tech to Curb Coronavirus Outbreak", The Straits Times:* https://www.straitstimes.com/asia/east-asia/how-china-s-korea-and-taiwan-are-using-tech-to-curb-outbreak
[77] *Kim, Max: "South Korea is Watching Quarantined Citizens With a Smartphone App", MIT Technology Review:* https://www.technologyreview.com/s/615329/coronavirus-south-korea-smartphone-app-quarantine/

data on the availability of protective masks[78]. The shortage of masks nationwide was resulting in long queues.

Case 2c: Public communication

Extensive use has been made of SMS notifications, as well as public information platforms, that includes public hotspot mapping. Pre-existing emergency infrastructure was also applied including the emergency ready app[79]. The communication measures have also emphasized on getting as many people as possible to report for testing, many in rapid "drive through" test stations. As of March 24, 2020, South Korea has capacity for **up to 20.000 tests a day – by far the most comprehensive testing regime worldwide.**

Figure 2 Emergency Ready App (*Source:*

Country study 3: Singapore

The Singapore public approach is characterized by **individual case tracing of contacts including the use of QR codes**[80] and making public exposure maps. In addition, it has taken a maximalist approach to testing and has segmented its quarantines into different risk levels. **What is remarkable is the strong emphasis on "public empowerment" and user-provided data given that** Singapore has some of the most elaborate surveillance infrastructures in the world. Singapore has highly integrated datasets and makes extensive use of data analytics in its policy making apparatus. In addition, Singapore is the third most surveilled city outside of China in terms of CCTV cameras and has likely also made use of artificial intelligence facial recognition software[81]. Singapore has also stimulated the use of public data API's to allow for app development and research.

Case 3a: Contact tracing and monitoring of infections[82]

Singapore has publicly applied phone-based travel data tracking in conjunction with CCTV to back-track infection vectors. It follows a similar trajectory to South Korea, with patient interviews and a review of CCTV footage. In so-called "close contact" or otherwise "difficult" cases the patients may be asked to **voluntarily provide their mobile phones so as to be able to extract historic GPS movement data** and retrace subjects' movements. What is unknown is the role of the provider-based cellphone tracking, which is widely believed to be extensive and likely can deliver at least as accurate results as used in Taiwan (see above). Also unknown is the use of facial recognition technology in analyzing CCTV footage, but Singapore

78 *Wray, Sarah: "South Korea to Step-Up Online Coronavirus Tracking", Smart Cities World:* https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109
79 *Jae-Un, Limb: "Emergency App Launched in English", Korea.net:* http://www.korea.net/NewsFocus/Sci-Tech/view?articleId=117966
80 *Singapore Government: "Coronavirus Disease 2019: Cases in Singapore", gov.sg:* https://www.gov.sg/article/covid-19-cases-in-singapore
81 *Aravindan, Aradhana & Geddie, John: "Singapore to Test Facial Recognition on Lampposts, Stoking Privacy Fears", Reuters:* https://www.reuters.com/article/us-singapore-surveillance/singapore-to-test-facial-recognition-on-lampposts-stoking-privacy-fears-idUSKBN1HK0RV
82 *Bengali, Shashank & Pierson, David: "How Singapore Has Kept the Coronavirus Under Control", Los Angeles Times:* https://www.latimes.com/world-nation/story/2020-03-11/a-singaporeans-view-of-the-coronavirus-its-surprising-to-see-the-u-s-so-messed-up

CCTV does have that capability[83]. Singapore has traced down every single infection and mapped the vector into social network visualizations[84].

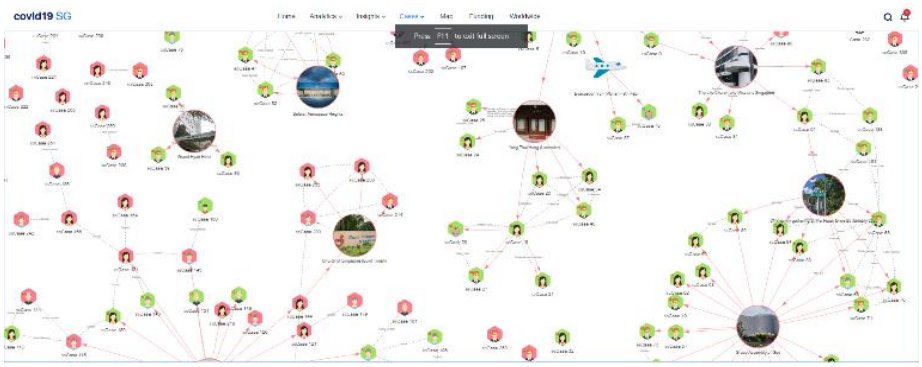

Figure 3 COVID19 Tracker (*Source: Strait Times)*

Figure 4 QR code for entry (*Source: Personal Communication)*

Singapore has put great public emphasis on the voluntary provider-based information. It has enforced checkpoints for any major office building that requires measurements by thermal scanner or digital thermometer, as well as logging of phone numbers and any recent travel in virus-affected areas. In addition, Singapore has made extensive use of QR codes at all public buildings and most transport nodes (including taxis) to facilitate contact tracing if needed. Using or entering these facilities require the scanning of the relevant QR code, and all public buildings have large-capacity body temperature measuring facilities (which is only marginally useful for this particular outbreak).

Singapore has also promoted "community" measures like the "TraceTogether" app. **TraceTogether is a government sponsored app** that uses Bluetooth to detect user proximity using the government developed BlueTrace protocol. Once a subject is confirmed to be infected anyone who has been within 2 meters for at least 30 minutes can be identified and notified[85]. The app does not track location or contacts and will only store the information for 21 days unless the subject is identified as a close contact.[86] The Singapore government has decided to provide the source code of the app for free for foreign adoption.[87]

Case 3b: Quarantine enforcement measures[88]

Two basic quarantine orders are issued. "Stay at home" orders are executed for any person who has travelled abroad or who was in a general coronavirus-positive area. They are required to stay at home for

[83] Interview
[84] *Covid 19 SG: "Singapore Cases", AgainstCovid19:* https://co.vid19.sg/cases
[85] *Baharudin, Hariz: "Coronavirus: S'pore Government to Make Its Contact-Tracing App Freely Available to Developers Worldwide", The Strait Times:* https://www.straitstimes.com/singapore/coronavirus-spore-government-to-make-its-contact-tracing-app-freely-available-to
[86] *Singapore Government: "Help Speed Up Contact Tracing With TraceTogether", Gov.sg:* https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether
[87] *Baharudin, Hariz: "Coronavirus: S'pore Government to Make Its Contact-Tracing App Freely Available to Developers Worldwide", The Strait Times:* https://www.straitstimes.com/singapore/coronavirus-spore-government-to-make-its-contact-tracing-app-freely-available-to
[88] *Min, Ang Hwee: "NTU to Log Student Attendence via QR Codes to Facilitate Contact Tracing for Coronavirus Outbreak if Needed", Channel News Asia:* https://www.channelnewsasia.com/news/singapore/wuhan-virus-ntu-contact-tracing-attendance-qr-codes-12422134

14 days. "Quarantine" orders are issued both or those who have tested positive for the virus or exhibited symptoms, as well as those who have been in close contact with an identified carrier[89] Quarantine may occur at home, but there are also dedicated government facilities available[90]. Both types of orders are mandatory and are enforced. Measures include twice-daily phone calls and cellphone images of their surroundings. If patients are found to be non-compliant, RFID tags or detainment and isolation are also implemented. Patients in home quarantine are sent a SMS at randomized times to report their current location through a link that is provided to monitor compliance.[91] While no public information is available on the use of cell phone (triangulation) data to monitor quarantine enforcement, it is likely that this is also used, similar to the employment in Taiwan.

Case 3c: Public communication[92]

Singapore has taken steps to publicly disclose all infection vectors as well as identify infection hotspots. These include daily announcements of individual infections by "cases" as well as their likely point of infection and subsequent movements on a public website. GovTech[93] has also provided two or three daily updates on WhatsApp to counter misinformation flows[94]; this included the application of AI tools to rapidly translate material from English into the other official languages.

Country study 4: China

The PRC is widely considered to have one of the world's most elaborate internal surveillance capacities using vast systems of artificial intelligence, CCTV and facial recognition technology, telecommunication monitoring (both Internet access as well as cell-phone location tracking) and comprehensive bio-metric data to keep track of its citizens. Many of these measures were already bundled together under the "Golden Shield" program.

Case 4a: Contact tracing and monitoring of infections[95]

The most well-documented case of app usage in China is the Alipay "Health Code" that uses color-coded QR systems for contact tracing and is effectively mandatory for any kind of movement. A Green QR code means proceed as normal, in the yellow and red cases means that there has been a definite or supposed contact with a identified coronavirus carrier. A green QR code is required to make use of public transportation, entering supermarkets or otherwise making use of public services, and it is necessary to "sign-in" with QR readers in specific locations. Data is intersected with other data streams including travel history as is the case in the "Qihoo 360/NoSugar Tech" proximity app[96]. AI applications including chatbots and automated

[89] *Yong, Clement: "How Quarantine Orders, Stay-Home Notices Differ", The Strait Times:* https://www.straitstimes.com/singapore/how-quarantine-orders-stay-home-notices-differ.
[90] *Ibid.*
[91] *Basu, Medha: "Exclusive: How Singapore Sends Daily Whatsapp Updates on Coronavirus", GovInsider:* https://govinsider.asia/innovation/singapore-coronavirus-whatsapp-covid19-open-government-products-govtech/
[92] *Ministry of Manpower:* https://www.mom.gov.sg/covid-19/advisory-on-social-distancing-measures
[93] *Government Technology Agency: "Our Role", GovTech:* https://www.tech.gov.sg/who-we-are/our-role/
[94] *Basu, Medha: "Exclusive: How Singapore Sends Daily Whatsapp Updates on Coronavirus", GovInsider:* https://govinsider.asia/innovation/singapore-coronavirus-whatsapp-covid19-open-government-products-govtech/
[95] *Mozur, Paul; Zhong, Raymond & Krolik, Aaron: "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", New York Times:* https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[96] *South China Morning Post: "Apps Check For Coronavirus", Abacus News:* https://www.abacusnews.com/tech/if-youre-worried-you-traveled-someone-coronavirus-get-these-apps/article/3048251

calls are made to survey travel history and response for the purpose of publicly identifying infection hotspots.[97] The app sends as well as receives data from government servers, leading to situations where suddenly a "health color" changes when a risk is identified by the system. It is widely presumed that user-delivered data is correlated with cellphone location monitoring data,[98] which however would be much less accurate and not useful in multistoried buildings with lots of traffic. A further app called "Fuxuema" ("back to school") created by Alipay competitor Tencent encourages the entry of student biometric data (like body temperature) to make yet another color-coded segmentation of risk. Other non-mandatory apps exist, such as another app provided by Tencent which tracks general "outbreak" areas (see Figure 6)[99] and therefore encourages users to avoid and plan around a specific area.

Figure 5 Alipay Health Code app (*Source: South China Morning Post)*

Figure 6 Tencent Mapping app (*Source: Tencent)*

Case 4b: Quarantine enforcement measures

Chinese quarantine protocols have been primarily centered on social containment through physical means rather than through technological means, a system massively facilitated by the use of local CCP officials and volunteers on a neighborhood level that are responsible for enforcing strict movement limitations in and out of residential buildings. The technological application has primarily been through the use of the "Health Code" app, which shows a red rating for all those under strictest quarantine measures. Software not used for enforcing quarantine per se, but which effectively still do so include "DingTalk", sometimes called the Chinese version of the popular communication program "Slack", which however also can include a location tracking component. It has become the principle quarantined schoolchildren home-school device and is especially unpopular as a result.[100] There are no public reports whether the Golden Shield system is being deployed to track quarantined user movement – for instance using cell phone location monitoring or facial recognition technologies. While this can be expected, the totality of the highly localized and physical travel restrictions in all urban areas make these technology measures less necessary.

[97] *Mehta, Ivan: "China's Coronavirus Detection App is Reportedly Sharing Citizen Data With Police", TNW:* https://thenextweb.com/china/2020/03/03/chinas-covid-19-app-reportedly-color-codes-people-and-shares-data-with-cops/
[98] *Kuo, Lily: "The New Normal: China's Excessive Coronavirus Public Monitoring Could be Here to Stay", The Guardian:* https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay
[99] *Yang, Samuel & Zhao, Iris: "Bid to Contain Coronavirus COVID-19 Sees Chinese Tech Giants Deploy Tracking Maps", ABC News:*https://www.abc.net.au/news/2020-02-22/coronavirus-covid-19-china-quarantine-measures-questioned/11987900
[100] *Li, Jane: "What is DingTalk, Alibaba's Slack Equivalent That Quarantined Kids in China Hate?", Quartz:* https://qz.com/1814937/what-is-dingtalk-the-alibaba-app-that-quarantined-kids-in-china-hate/

Furthermore, an app has been rolled out that allows you to check not only your own exposure risk, but also the risk of three other persons.[101] The assessment is based on shared classrooms, housing, travel, and the health status of first-degree social contacts upon which an evaluation of risk is made. The app is ostensibly connected into the data streams of the National Health Commission, the Ministry of Transport, China Railway, and the Civil Aviation Administration of China. The app appeared to be successful in calming down public anxiety and has been copied in South Korean cities.[102] On the mitigation side, various apps allow users to identify whether they have traveled on a flight or train with another person who was infected with the virus. Similar apps exist for mapping of corona indications, including by Tencent (see Figure 6).

Case 4c: Public communication

The government has used the Golden Shield and Great Firewall technologies to both limit outside information as well as help track "misinformation" of whatever description. The "counter misinformation" track has been particularly challenged due to the overall high amount of communication by Chinese during the crisis, but had already failed at the outset – when the "whistleblowing" Wuhan doctor Li Wenliang posted a social media alert to his colleagues on the virus on December 30th. The report went viral despite attempts to shut it down. There has also been a marked uptick in the activity of the so-called "50 cent army", the CCP's 2 million strong "commentator force" whose job previously was largely to distract from political issues. Since March 15, it has directly contributed to spreading rumors that "the US Army was responsible for the Wuhan outbreak".[103]

Country study 5: Israel

The Israeli government – in the middle of a prolonged leadership dispute – announced on March 18 an emergency law to allow for the use of the country's comprehensive domestic surveillance apparatus to combat the spread of the coronavirus.[104] While relatively new, these measures likely draw from the high level of integration between telecom providers as well as various datasets held by parts of the government. While the means are very controversial in Israel itself, a number of other CTQ apps are being developed as well.

Case 5a: Contact tracing and monitoring of infections

On March 18, some Israeli recipients received a SMS message from the Health Ministry announcing they had been in close contact with a coronavirus case and were told to self-isolate immediately. It subsequently emerged that the internal security service Shin Bet was using the technologies associated with counterterrorism to track and identify possible carriers based on past cellphone geolocations. While little additional information has been revealed, subsequent reporting indicates that the telephone providers have been able to fully map individual cellphone user movements at a very high level of detail (possibly

[101] *The Strait Times: "Coronavirus: China Introduces Close Contact Detection App":* https://www.straitstimes.com/asia/east-asia/coronavirus-china-introduces-close-contact-detection-app
[102] *Watson, Ivan & Jeong, Sophie: "Coronavirus Mobile Apps are Surging in Popularity in South Korea", CNN:* https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html
[103] Yu, Haiqing: *"The coronavirus and Chinese social media: finger-pointing in the post-truth era"*, The Conversation: https://theconversation.com/the-coronavirus-and-chinese-social-media-finger-pointing-in-the-post-truth-era-130698.
[104] *Lomas, Natasha: "Israel Passes Emergency Law to Use Mobile Data for COVID-19 Contact Tracing", TechCrunch:* https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/

exceeding the 30m location radius given as a normal maximum with different GSM triangulation technologies) over previous weeks and have combined the data with Health Ministry data on known COVID-19 carriers.[105]

On March 22, the Israeli Health Ministry launched the "HaMagen" app, Hebrew for "The Shield". The voluntary app uses a phone's location history over the past 14 days and cross-references it with data from the epidemiological investigations of existing cases to determine if close contact was made.[106] It is unknown from where the original data on the investigation is drawn from.

Case 5b: Quarantine enforcement measures

Media reporting indicates that the same Shin Bet surveillance infrastructure was being used to provide real-time information to law enforcement on the street tracking adherence to quarantine orders. It was reported that it can extend to individual vehicles being stopped on the suspicion that a passenger is a likely or potential carrier who should be in quarantine.[107] At the same time, the government has said that it would not use the geolocation system to enforce quarantine procedures.[108]

[105] *Estrin, Daniel: "Israel Begins Tracking and Texting Those Possibly Exposed tot he Coronavirus", NPR:* https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus
[106] *Kahan, Raphael: "Israeli Health Ministry Launches Voluntary Covid-19 Tracking App", CTech:* https://www.calcalistech.com/ctech/articles/0,7340,L-3803052,00.html
[107] *Estrin, Daniel: "Israel Begins Tracking and Texting Those Possibly Exposed tot he Coronavirus", NPR:* https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus
[108] *Gross, Judah Ari: "Netanyahu Sparks Privacy Scare With Move to Track Corona Patient's Phones", The Times of Israel:* https://www.timesofisrael.com/netanyahu-sparks-privacy-concerns-with-move-to-track-corona-patients-phones/

Appendix B: Tracking through Technology

The overall goal of industry data tracking is to create and connect as many data points about a consumer that results in a detailed behavioral profile, which in turn can reveal demographics, interests, health, purchasing habits and locations, for targeted advertising purposes. Companies such as Google and Facebook then share this data with advertisers in an auction for add space, known as real-time bidding.[109] Both companies are also largely dependent on the same data to help maintain and optimize their services – using it, for instance, to route Internet traffic as well as decide what content is to be shown to whom at what time. In some cases, the marketing requirements and the operational requirements are indistinguishable, which has created legal loopholes that have commonly been exploited in the past.

Data collection: First-party data & third-party data

Companies such as Facebook and Google collect data directly from their customers through their own products and services – known as ***first-party data***.[110] Google's services and products covers about 62% of mobile bowsers[111], 69% of desktop browsers[112], and the operating systems on 71% of mobile devices[113]. Moreover, 92% of Internet searches go through Google[114], and it runs code on approximately 85% of sites on the Internet[115] and inside as many as 94% of apps in the Play Store.[116] They also collect information about individuals not using their services.[117] Furthermore, there is an entire ecosystem of advertisers, brokers, and other companies that collect data (see Figure 8) – known as ***third-party tracking***.[118]

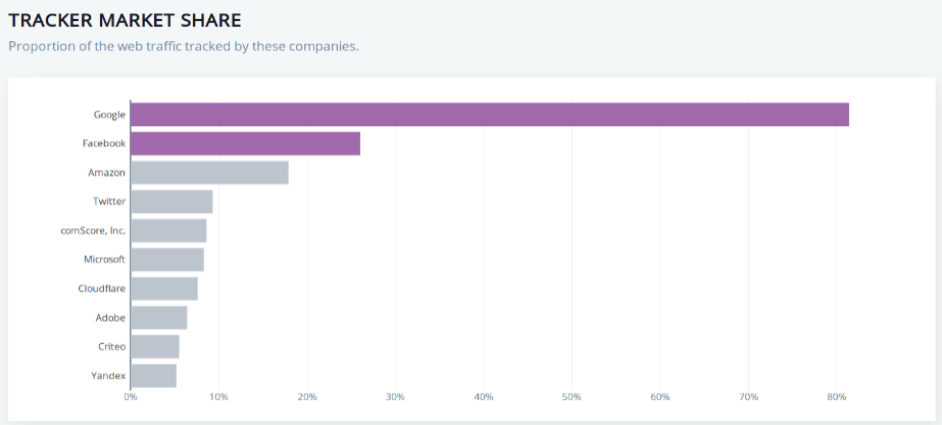

Figure 7 Top trackers on the Web, ranked by the proportion of web traffic that they collect data from. *(Source: WhoTracks.me)*

[109] *Cyphers, Bennett: "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance", EFF:* https://www.eff.org/wp/behind-the-one-way-mirror#firstvsthird
[110] *Ibid.*
[111] *Stat Counter Worldwide: "Mobile Browser Market Share Worldwide", GS Stat Counter:* https://gs.statcounter.com/browser-market-share/mobile/worldwide
[112] *Stat Counter Worldwide: "DesktopBrows Market Share Worldwide", GS Stat Counter:* https://gs.statcounter.com/browser-market-share/desktop/worldwide
[113] *Net Marketshare: "Operating System Market Share":* https://www.netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Mobile%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22platform%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22platformsMobile%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222019-02%22%2C%22dateEnd%22%3A%222020-01%22%2C%22segments%22%3A%22-1000%22%7D
[114] *Stat Counter Worldwide: "Search Engine Market Share Worldwide", GS Stat Counter:* https://gs.statcounter.com/search-engine-market-share
[115] *W3 Techs: "Usage Statistics and Market Share of Google Analytics for Websites":* https://w3techs.com/technologies/details/ta-googleanalytics
[116] *Clement, J.: "Leading Mobile Android App Ad Networks SDKs 2020", Statista:* https://www.statista.com/statistics/1035623/leading-mobile-app-ad-network-sdks-android/
[117] Facebook, for example, does so through its invisible 'pixel': https://developers.facebook.com/docs/facebook-pixel/implementation/conversion-tracking/;
[118] Wolfie Christl: *"Corporate Surveillance in Everyday Life How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions"* Cracked Labs Vienna.

Data identifiers: Linking data to people

In order to link data to people, *identifiers* are used. *Identifiers* are characterized as unique, persistent, and available, which are used to link data to a person through such mediums as:[119]

- **Web identifiers**: Cookies, IP address[120], Transport Layer Security (TLS) state[121], local storage super cookie and iframes[122], browser fingerprinting[123];
- **Mobile identifiers**: Phone number[124], IMSI[125] and IMEI[126] number, advertising ID[127], Media Access Control (MAC) address[128], mobile fingerprinting;
- **Real-world identifiers**: license plates[129], face biometrics[130], credit card numbers.

Mobile identifiers differ because of the integration of apps that usually require a log-in with an account that already functions as an identifier, making it easier for these companies to profile user identity and behavior. Most mobile tracking happens through third-party software kits (SDKs) often developed by Google or Facebook, which developers include in their app. Unlike web identifiers, there are no first-party and third-party resources in mobile identifiers. Multiple identifiers are often used together and, in some cases, anonymized data can still be linked to a specific individual.[131]

[119] Derived from: *Cyphers, Bennett: "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance", EFF:* https://www.eff.org/wp/behind-the-one-way-mirror#firstvsthird. This report includes a detailed description of the identifiers.
[120] IP addresses can be spoofed through a VPN or Tor. While an IP address is only temporary (days to months), it can be used to create to long-term profiles, including mapping relationships between devices: http://pages.cs.wisc.edu/~pb/kdd17_final.pdf
[121] TLS session IDs and session tickets only last for hours-days but are unique cryptographic identifiers that help speed up encrypted TLS connections. Sy, Erik et. al: *"Tracking Users across the Web via TLS Session Resumption", Cornell University:* https://arxiv.org/abs/1810.07304
[122] Iframes offer a way for websites and third-party domains (website in a website – such as embedded Youtube videos) to store data in a browser for longer periods of time.
[123] Fingerprinting is a complex tracking method using one or more attributes, such as screen resolution, software packages installed, time zone, to identify an individual browser or device. Folwer, Geoffrey A.: *"Think you're anonymous online? A third of popular websites are 'fingerprinting' you*.", The Washington Post: https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/; Chen, Brian X.: *"'Fingerprinting' to Track Us Online Is on the Rise. Here's What to Do."* The New York Times: https://www.nytimes.com/2019/07/03/technology/personaltech/fingerprinting-track-devices-what-to-do.html
[124] Phone numbers on android are only available to third-party trackers in apps that have been granted certain permissions. iOS prevents apps from accessing a user's phone number.
[125] Every mobile device connected to a mobile network is assigned a unique identifier called an International Mobile Subscriber Identity (IMSI) number by their mobile carriers and stored on SIM cards. This number is shared with the mobile provider every time someone connects to a cell tower – which is always. This can be used to track your location.
[126] Every mobile device has an International Mobile Equipment Identity (IMEI) number "baked" into the hardware. You can change your SIM card and your phone number, but you can't change your IMEI without buying a new device.
[127] Much like a cookie, an advertising ID is a identifier for a mobile device that is built into iOS and Android operating systems for the purpose of helping behavioral advertisers link user activity across apps on a device. These IDs can be changed and in iOS turned off.
[128] MAC addresses are hardware identifiers used by devices that can connect to the Internet to set up the connection between two wireless-capable devices over Wi-Fi or Bluetooth. While websites don't see this address, any nearby networking device can pick up on the probe requests, including beacons that can track users' movement around and can also identify when two people are in the same location and use that information to build a social graph. *MAC address randomization* creates spoofed addresses and is a default setting in both iOS and Android.
[129] Automatic license plate readers (ALPRs) are special-purpose cameras that can automatically identify and record license plate numbers. Databases may be maintained by law enforcement or companies. More information available on: https://www.efforg/pages/automated-license-plate-readers-alpr
[130] Facial recognition is at the beginning of its implementation and impact and still prone to errors: https://www.perpetuallineup.org/
[131] *Ohm, Paul: "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", UCLA Law Review:* https://www.uclalawreview.org/pdf/57-6-3.pdf; *Barbaro, Michael & Zeller, Tom: "A Face is Exposed for AOL Searcher NO. 4417749", New York Times:* https://www.nytimes.com/2006/08/09/technology/09aol.html

Geolocation tracking

Four categories of geolocation tracking are identified:[132]

1. **Mobile signal tracking through cell towers**, also known as **triangulation,** includes the *IMSI number* as an identifier.[133] Governments have and continue to request this kind of information through "tower dumps" – a record of all the mobile devices that were present in a certain area at a certain time.[134] Carriers also exchange this location data.[135] Its accuracy depends on many factors, including the operator's technology and the number of cell towers they have in an area. It ranges from around 50 to 100m in optimal conditions and to several kilometers in rural areas (see the explanation of workings of TDOA below).[136] However, using a specific protocols originally developed to support US 911 services – the Radio Resource Location Protocol (RRLP) – it is possible to get much more accurate measurements, possibly comparable to GPS accuracy.[137] Also, using so-called baseband attacks some carriers might have the possibility to exploit the known weaknesses of the SS7 GSM protocol, meaning that the actual GPS data generated by the phone may also be gathered directly - leading to accuracy of up to 5m.
2. **Mobile signal tracking through cell tower simulators:** these portable cell phone towers, also known as an IMSI Catcher or Stingray, finds devices through the IMSI and other device properties.[138] Some stingray devices have a range of "several kilometers"[139], and "by collecting the signaling information from several locations, the system can triangulate the location of the phone more precisely."[140] IMSI catchers can be used instead of cell towers, but it is possible to use them in conjunction as well.
3. **Wi-Fi and Bluetooth tracking:** in contrast to mobile networks, Wi-Fi and Bluetooth can normally be received only within a short distance. However, there have been cases where these signals can still be received from a distance up to 382km under rural conditions with little radio interference.[141] Wi-Fi location tracking systems should be able to give a high level of accuracy ranging from 3-5m[142], or even less.[143] Both signals include the *MAC address* as identifier, which can be observed even if a device is not actively connected to the respective wireless network unless Wi-Fi and Bluetooth are completely

[132] Derived from: *EFF: Surveillance Self-Defense: "The Problem With Mobile Phones":* https://ssd.eff.org/en/module/problem-mobile-phones. For a visualization of the tracking techniques, visit: https://www.washingtonpost.com/wp-srv/special/national/cell-phone-tracking/. For an example of the personal implications, see the case of Malte Spitz, who requested data from his mobile operator in 2010: Biermann, Kai: "*Betrayed by your own data*" , Zeit Online: https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz.

[133] *O'Brien, Ciara: "How Your Smartphone Makes it Easier to Track Your Movements", Irish Times:* https://www.irishtimes.com/business/technology/how-your-smartphone-makes-it-easier-to-track-your-movements-1.3722961

[134] *Williams, Katie Bo: "Verizon Reports Spike in Government Requests for Cell 'Tower Dumps'", The Hill:* https://thehill.com/policy/national-security/347800-government-requests-for-cell-tower-dumps-spikes-verizon

[135] *Timberg, Craig: "For Sale: Systems That Can Secretly Track Where Cellphone Users Go Around the Globe", Washington Post:* https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

[136] *EFF: Surveillance Self-Defense: "The Problem With Mobile Phones":* https://ssd.eff.org/en/module/problem-mobile-phones

[137] *Radio Resource Location Service Protocol: "Mobile (In)Security":* https://projects.osmocom.org/projects/security/wiki/RRLP

[138] *EFF: "Street-Level Surveillance":* https://www.eff.org/nl/pages/cell-site-simulatorsimsi-catchers ; *Yomna, N.: "Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks", EFF:* https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

[139] *Fakhoury, Hanni: "Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About":* eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy

[140] *Valentino-DeVries, Jennifer: How 'Stingray' Devices Work", Wall Street Journal:* https://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/

[141] *EFF: Surveillance Self-Defense: "The Problem With Mobile Phones":* https://ssd.eff.org/en/module/problem-mobile-phones

[142] In order to reach this level of accuracy, you need to be able to triangulate (so have at least three access points) and use time difference of arrival (TDOA) measurements with wide bandwidth. https://www.airfinder.com/blog/wifi-location-tracking

[143] *Simonite, Tom: "Wi-Fi Trick Gives Devices Super-Accurate Indoor Location Fixes", MIT Technology Review:* https://www.technologyreview.com/s/542561/wi-fi-trick-gives-devices-super-accurate-indoor-location-fixes/; http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p269.pdf

[143] *EFF: Surveillance Self-Defense: "The Problem With Mobile Phones":* https://ssd.eff.org/en/module/problem-mobile-phones

turned off.[144] Because of its limited range and high accuracy, this method is more appropriate for short-distance applications (e.g. pinpointing the time and location people enter or leave a specific building). However, it is possible to combine a smartphone's Wi-Fi and Bluetooth signal reading together with data from cell towers to achieve a "high level" of accuracy as well.

4. **Location information through Apps and Web browsing (determined via GPS):** GPS allows phones to determine their location through the signals transmitted by a GPS satellite. The satellite is merely the transmitter of signals and the phone is the actual receiver. Tracking in this case is done through apps that ask for the phone's location determined via GPS. Map apps, for example, determine location based on the cell phone towers and/or GPS. Some of these apps will then transmit said location over the network to a service provider, which, in turn, provides a way for other people to track the individual's location. Normally a telecom provider will not have access to this data, although in the past it was reported that some phones could be "tricked" to provide GPS data to the provider. Non-military GPS (as used by smartphones) usually has a maximum accuracy of 5m.

Time Difference of Arrival (TDOA), also known as **multilateration**, is a technique used for the geolocation of a radio-frequency (RF) transmitter. Using three or more receivers, TDOA algorithms locate a signal course from the different arrival times at the receivers. According to one source, "TDOA geolocation results can give locations with *as little as* ten meters of uncertainty. Unlike other geolocation techniques, TDOA can provide accurate geolocation even for signals with power levels below the noise floor."[145] A distinction is made between U-TDOA and OTDOA.[146] Both depend on TDOA measurements and both are applicable to Universal Mobile Telecommunications Systems (UMTS). Uplink Time Difference of Arrival (U-TDOA) is a network-based positioning method and can be described as "a wireless location technique that compares the time difference of mobile phone signals as they reach multiple location measurements units (LMUs)."[147] U-TDOA was proposed by TruePosition as a new approach to the original OTDOA (a handset based positioning method working on the Downlink channel) to overcome the hearability problem.

In each case, location tracking is not only relevant to find where someone is right now, but also where and with who they have been in the past. The Snowden leak, for example, showed that the NSA was tracking cellphone locations worldwide by tapping into the cables that connect mobile networks globally.[148] More recently, U.S. Federal agencies like ICE have bought access to commercial databases for app-generated location data for the purpose of immigration and border enforcement.[149] This bring us to the contentious data sharing ecosystem of real-time bidding.

[144] Ibid.
[145] *CRFS: "How Accurate is TDOA Geolocation?":* https://www.crfs.com/blog/how-accurate-tdoa-geolocation/. A number of factors limit the accuracy of TDOA, including timing accuracy, sample rate and bandwidth, signal periodicity, network geometry, or obstacles.
[146] For more details visit: https://www.etsi.org/deliver/etsi_ts/125300_125399/125305/07.01.00_60/ts_125305v070100p.pdf
[147] "TruePosition describes U-TDOA as follows: "it uses LMUs located at the base stations to calculate the time difference measurements used to determine the location of the mobile phone. The operator's network makes a location request to the Wireless Location Gateway (WLG), which routes the request along the mobile phone's channel assignment to the Wireless Location Processor (WLP). The request is transmitted through the wireless operator's network and then routed back to the WLG and the WLP. The WLP instructs the LMUs to listen for a signal. The LMUs measure the time difference of arrival of a mobile phone's signal and send the measurements to the WLP. The WLP calculates the mobile phone's location by determining the difference in the times the signal arrived at multiple LMUs. The WLG forwards the location to the operator's network or the requesting application." From https://ecfsapi.fcc.gov/file/7020038703.pdf.
[148] *Gellman, Barton & Soltani, Ashkan: "NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show", The Washington Post:* https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
[149] *Tau, Byron & Hackman, Michelle: "Federal Agencies Use Cellphone Location Data for Immigration Enforcement", Wall Street Journal:* https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

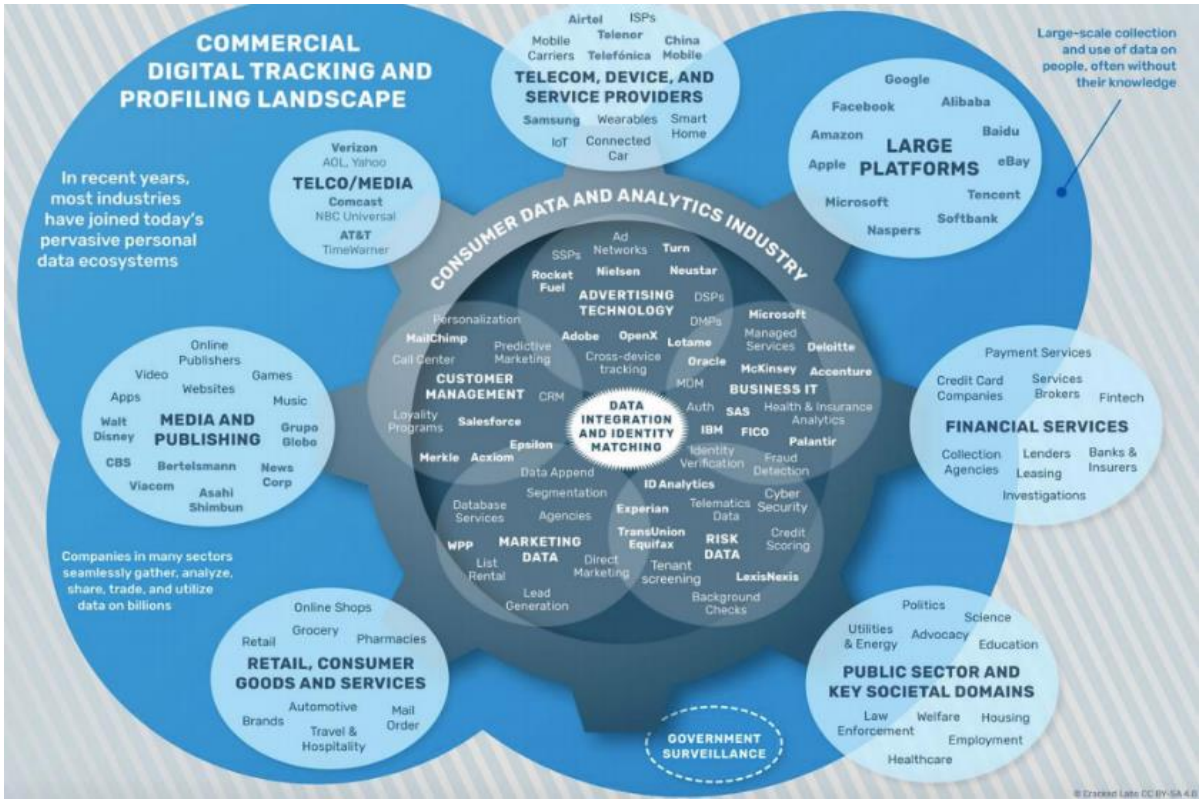

Figure 8 Mapping the commercial digital tracking and profiling landscape (Source: Wolfie Christl: "Corporate Surveillance in Everyday Life How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions" (Cracked Labs Vienna, June 2017)).

Data sharing and selling: Real-time bidding

In order to come closer to the goal of establishing sophisticated customer profiles, companies need more than just first-party tracking. The information each company has only offers one or more piece(s) of the puzzle. When shared with others, the data-points in the profiles expand into a bigger network. Data sharing and mainly takes place through real-time bidding (RTB) – a data collection and sharing system that enables profiling by advertisers, data brokers, hedge funds and others. It is the process by which publishers, such as Google and Facebook, auction ad space in milliseconds. In doing so, they collect personal information, merge it into a sophisticated profile, and share sensitive information with others —including geolocation, device IDs, identifying cookies, and browsing history.[150] During the RTB process, companies sync the targeted profile with any information they or data brokers have on the profile to decide how much to bid for the ad impression. When a user visits the page via the add, the RTB participants harvest additional information from this user that is injected into their profile. Thus, RTB is both a cause of tracking and a means of tracking. Google controls a sizeable share of nearly every level of the RTB ecosystem – the supply-side platforms that collect user data, ad exchanges that function as auctioneers, and demand-side platforms that bid on behalf of advertisers.[151]

[150] *Cyphers, Bennett: "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance", EFF:* https://www.eff.org/wp/behind-the-one-way-mirror#firstvsthird

[151] For example, in 2007, Google acquired ad network DoubleClick (web-based) and in 2009 it acquired AdMob (adds for mobile apps).