Ethical AI and Big Data in Times of Pandemic

Merve Hickok
aiEthicist.org

In times of public emergencies or security threats, governments put in place practices to gain information, hence control and authority, under the premise of responding to crisis. These programs incur longer term unintended consequences. We review the surveillance and tracking put into effect during COVID-19 pandemic and overlay it with ethical Big Data and AI principles of Purpose & Value, Accountability & Trust, Respect for Data Rights & Privacy, and Prevention of Harm and Bias. Exigent circumstances must not lead us down the road of trading ethics for techniques and technologies that impact democracy under the guise of 'public health'.

Keywords: artificial intelligence, ethics, applied ethics, AI and ethics, surveillance

INTRODUCTION

These last few weeks [April 2020], have you gone through a single waking hour where you have not heard the word "corona virus", thought about it, or been impacted at home or work because of it? That is how big the impact of this novel virus has been on the fabric of our personal and professional lives.

It also showed us how vulnerable everything is, everything we had taken for granted: our health, jobs, investments, connections, freedoms, privacy — just to name a few. It is times of crisis like this where we think more about these concepts and question their applications. It is also times like this where our lives are in a potential danger that our sense of ethics, humanity and morality is tested.

There is probably no one in the world right now who does not appreciate the health workers, their commitment and personal sacrifices to fight the virus. These novel situations are forcing medical institutions and staff to make very tough ethical decisions daily. We also have a huge appreciation for every single organization and person that is working to keep us going and / or re-purposing their work. Demanding times fire innovation. Demanding times also fire extraordinary measures. It is not the intention of this article to discuss the medical and clinical ethics in times of public health.

This article instead expands on the practices of surveillance and tracking methods that became part of our lives overnight and overlays it with the ethical Big Data and AI principles to suggest practices to protect our privacy and rights while still fighting an unprecedented fight against a pandemic.

FALSE DICHOTOMY

In times of major crises or security attacks, governments and authorities tend to put in place certain programs and practices that would help them gain more information and hence control and authority over populations under the guise of responding to an emergency. These programs and practices often incur longer term unintended consequences. If you are reading this in America, your mind immediately makes a connection with this sentence with the post 9/11 intelligence and surveillance programs that were rolled out. Then the suggestion was to forgo some of your privacy in return for your safety, but this was supposed to be a trade-off of limited duration. This was why the surveillance laws associated with the USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) required regular reviews and renewals and had sunset clauses. However even with those regular reviews and even with the passage of the USA Freedom Act in 2015 that rolled back a lot of the provisions of the Patriot Act, parts of that surveillance law are still intact and still hotly debated.

Today, the suggestion is to forgo your privacy so that the pandemic can be contained, and we can keep the public healthy and alive. There would be no discussion about this suggestion if the dichotomy was a correct one. However, when we are talking about using big data and massive tracking methods to trace contact among members of the population, for example through cell phone location usage, or collecting retail and consumption data and packaging to trace and stop the pandemic, then we are talking about a false dichotomy. Yes, there is a very compelling need for data collection and use of technology in times of a pandemic but we need to remember in our debate that even as we speak there is still no mass production and deployment of virus testing across US that would enable the agencies map all the cases and impose measures to contain them. We do not know everyone who actually has it and continues to spread it. Knowing who is infected should be the first and foremost step. In the absence of effective and mass testing, the dataset is incomplete and inaccurate to start with and the outputs from the models on whether any of the current measures are working are also hence incomplete and inaccurate. The virus is spreading because people have been unwilling to take basic universal hygiene precautions; because when required by public health authorities we have been unwilling to physically distance ourselves; because governments have put their political biases ahead of what science and data tells them; because whether it is at federal, state, local or company level there was not enough planning and timely actions to get ahead of the problem…and I am afraid people will lose their trust in authorities soon and ignore the guidelines altogether. So, let's not put this on lack of surveillance methods and suggest that everything would be solved if only we know what every individual did around the clock.

We need data and data-based decisions more than ever these days. However, we should also remember that it is a very sensitive balancing act to protect individual privacy and human rights at one hand and collect information that is critical to the public good and public health on the other. It does not mean that it is impossible, or that we cannot use technologically ethically. We must find ways to slow the spread and save lives without infringing on liberties and risking our future. What we do today as individuals, organizations or governments, that's how we will be remembered in the future. That is what we will remember ourselves when we look back to these days.

Just like Elizabeth Renieris (Renieris, 2020), a fellow at Berkman Klein Center for Internet & Society at Harvard said "While no one seriously questions the need for interventions that can protect public health and safety, the framing of many privacy-related concerns skips a fundamental step in the analysis — namely, asking when an interference with fundamental rights is justified. This analysis is grounded in core principles of international human rights law…If the privacy community skips this critical step, we have already lost the battle to protect our fundamental rights."

Hu Yong (Hao, 2020), a professor at Peking University's School of Journalism and Communication recently wrote "You might as well ask yourself, has history ever shown that once the government has surveillance tools, it will maintain modesty and caution when using them?" The answer is the same whichever country you put under scrutiny. In addition to the government's own efforts, we should also ask the same question about the private companies and whether they would maintain modesty and caution. In the span of a few weeks we have come across a number of applications used for surveillance that we would have called unacceptable or draconian from a privacy or freedom perspective if it was not for the pandemic that we are living through.

Here are some examples of how some countries rolled out big data and surveillance methods so far as part of the pandemic response:

- *In England, anonymized data from the telecom provider O2 was shared with authorities to determine the extent to which the populace had implemented social distancing (Martin, 2020).*
- *In addition to already starting partnerships with CDC in US and NHS in UK, according to a new report from Bloomberg (Fouquet & Torsoli, 2020) Palantir is also pitching its analytics software to government officials in France, Germany, Switzerland and Austria. Palantir, a company that counts CIA among its investors, is apparently pitching both its Foundry software and a tool called Gotham, which is best-known for helping intelligence and law enforcement agencies (Hatmaker, 2019) track individuals, as in* the case of the company's work with ICE *(Ongweso Jr, 2020). Those two tools are being proposed to European health agencies as a blended solution that could help countries get a bird's-eye view of the pandemic.*
- *In Israel, Shin Bet internal security service uses the anti-terrorism technology to tap into cellular data to retrace the movements of people infected by COVID-19 (Lubell, 2020).*
- *In China, the measures include phone tracking, facial recognition, and requiring hundreds of millions of citizens in lock-down to download an app to categorize their risk (Mozur, 2020)*
- *In Taiwan, authorities have deployed an "electronic fence" around quarantined households that alert police if citizens under quarantine leave the home or even turn off their phones (Newton, 2020)*
- *In South Korea an app, developed by the Ministry of the Interior and Safety, allows those who have been ordered not to leave home to stay in contact with case workers and report on their progress. It uses GPS location tracking to make sure they are not breaking their quarantine. Those in lock-down are assigned to a local government case officer, who checks in twice a day by phone to track the development of any symptoms, and mobile testing teams are deployed to collect samples if things escalate. Those in quarantine can use the app to report their symptoms and provide status updates to officials. And if they venture outside their designated quarantine area, an alert will be sent to both the subject and the case officer. "Citizens were provided with an explanation of what information was collected, for what purpose and when it would be erased,". However, this does not prevent the government sending "safety guidance texts" that could expose individual's private lives and fuel social stigma. The saving grace in South Korea is that it was able to quickly deploy rapid and mass testing for its population, so it is actually using the tracking as a second measure after testing. (Max, 2020)*
- *In Iran, a coronavirus app, named AC19, released by the Ministry of Health encourages users to install the app, and complete a test to see if they had symptoms of coronavirus (Chrysaidos, 2020). The app sends the user location and all the other information entered by the user (mobile number, gender, name, height, etc) back to the developer's server. The developer company, named Smart Land Strategy, previously built two Telegram clones named Gold Telegram and HotGram (Cimpanu, 2020). Both apps were removed from the Play Store on accusations of secretly collecting user data, and reports at the time claimed the apps were developed at the behest of Iranian intelligence agencies*
- *Hong Kong is using electronic wristbands connected to a phone app as part of its effort to enforce quarantines and reduce the spread of the new coronavirus. All passengers arriving must wear the wristbands and share their location with the government via messaging platforms, like WeChat and WhatsApp (Saiidi, 2020)*
- *In Poland, the government has reportedly rolled out an app to ensure compliance with home quarantining. It requires for citizens to upload time-stamped selfies that are then verified using facial recognition and location data (Amnesty International, 2020).*
- *In US, White House announced that it is in talks with tech companies to use location data to track and analyze social distancing implementation although more detail on the privacy*

aspect of the technology is still nowhere on the horizon (Romm, Dwoskin & Timberg, 2020). As of the time of writing this article, we are still not sure what those talks entailed.

When organizations and researchers are trying to come up with solutions and when time might be considered a luxury, quick deployments may not always go through many of the checks and guidelines that might be in place for ethical and unbiased, responsible use of AI. However, that is exactly the wrong kind of trade-off we should accept. “We need to keep in mind that the big ethical challenges around privacy, accountability, bias, and transparency of artificial intelligence remain,” said Kay Firth-Butterfield (Hao, 2020), WEF’s head of artificial intelligence and machine learning in response to recent developments.

This point was also underlined at the Future of Privacy’s Virtual Workshop with ethicists, academics, government officials, and corporate leaders discussing the responsible data sharing in times of crisis (Ringrose, 2020). One of the advices coming out of this workshop was that entities should continue to follow their guidelines for data protection during the crisis and recognize that their standards for sharing have not changed. The agreement was that standards for prioritizing review of projects have changed because of pandemic-driven urgency, however data protection principles should not be abandoned because there is a crisis.

Referencing back to the memories of 9/11 again, the Commission Report also had recommendations to ensure that crisis should not preclude discussions of ethics — “The U.S. government must define what the message is, what it stands for. We should offer an example of moral leadership in the world, committed to treat people humanely, abide by the rule of law, and be generous and caring to our neighbors…We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America’s liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.”

I am not suggesting that tech companies are opportunistic giants here. I can only imagine how much these leading companies, with their incomparable infrastructure, data and developers are being pressured for data and support from governments and health agencies. I am usually a big critic but at least in the case of a pandemic, I would like to give them the benefit of doubt, especially when people’s lives and livelihoods are in the line. But I am also in agreement with Jules Polonetsky CEO Future of Privacy Forum, when he says that “Tech should follow here. Follow the guidance of non-tech experts by supporting epidemiologists, public health experts and safety experts in every way they need, consistent with civil liberties. Help those leaders communicate to the public and with each other, design what they need” (Polonetsky, 2020).

CORE PRINCIPLES OF ETHICAL AI AND BIG DATA

So how can we ensure that AI ethics guidelines are still what guides us when these new models and technology are being created and deployed in quick order? Let’s remember some of the core principles of ethical AI and big data and how these might be impacted during a pandemic.

Purpose & Value

The US government, just like many other governments, would normally need to obtain users’ permission or court orders to obtain user data from network providers or software companies like Google and Facebook. However, in times of emergency or national security the powers are broadened in pretty much every country. The public-private partnerships in these times can provide governments with data that they would not otherwise have.

We all want more data in our lives — for the decisions we need to make as well as the decisions that are made about us. However, we need to differentiate what we would like to have from what we really need to have to solve a specific problem. “What’s really important is for the government to be really clear in articulating what specific public health goals it’s seeking to accomplish,” says Kelsey Finch (Fussell, 2020), senior counsel at the Future of Privacy Forum. “Public health programs should therefore use means that are the least coercive necessary to meet important public health goals and should be proportionate to the health risk being addressed. Where individual consent for restrictive or coercive measures is not possible, states should use transparent and accountable decision-making processes."

Proportionality principle applies whereby the least intrusive solutions should always be preferred, considering the specific purpose to be achieved. As European Data Protection Board states, invasive measures, such as the "tracking" of individuals could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing (EDPB, 2020). However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles.

These are not nice to haves. If we are rolling out such massive measures and technology, we need clearly defined purpose that is also explained to the public, and all the data collected within this scope & time limit must be retained only for an agreed time frame.

In US, one of the most applicable safeguards in relation to information sharing and privacy comes from the Attorney General's Guidance Implementing Federal Statutes relevant in the Information Sharing Environment (Department of Justice, 2008) that addresses the Privacy Act. It requires federal law enforcement to "assure that civil liberties and privacy are protected throughout any assessment or investigative process…conduct no investigations based solely upon one's exercise of First Amendment activities (the free exercise of speech, religion, assembly, press or petition) or on the race, ethnicity, national origin or religion of the subject…and provides six basic principles. One of these principles is to "Only investigate for a proper purpose" and the other is to "employ the least intrusive …(particularly if there is the potential to interfere with protected speech and association, damage someone's reputation, intrude on privacy, or interfere with the sovereignty of foreign governments)". The same guidance also specifically refers to the Privacy Act of 1974 (5 U.S.C. § 552a) as balancing the government's need for information with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from the government's use, collection, maintenance and dissemination of that information. These principle mandate that the government transition from least intrusive methods to more intrusive methods over the course of an investigation while judicial oversight of these methods increases at the same time.

There are huge benefits collecting data and making data-based decisions. However especially in times like these where resources are getting scarcer and the focus should be on solutions that work, we should focus on work that will help the public health — not on practices that will make some people / organizations more powerful. Looking at some of the surveillance and contact tracking methods used in different countries, we should ask ourselves if these methods actually achieve the purpose, if there is real value in implementing them. Currently the public and private initiatives are collecting and combining location data, financial transactions, consumption patterns, health data and social media interactions. Of course, the private companies and data brokers have been doing this for ages. However, this does not justify the current massive surge of surveillance techniques in the name of 'public health'. We need to answer honestly the question of why we are collecting these and whether what we are doing really helps public health, or are we testing methods for the sake of testing the methods and technology and how far we can stretch people's acceptance of privacy erosion. Are these surveillance techniques and models actually changing any behavior on the public's response to the pandemic? Are they making people listen to the guidelines coming from public health authorities?

"The seduction of these consumer products is so powerful that it blinds us to the possibility that there is another way to get the benefits of the technology without the invasion of privacy. But there is," said William Staples, founding director of the Surveillance Studies Research Center at the University of Kansas. "All the companies collecting this location information act as what I have called Tiny Brothers, using a variety of data sponges to engage in everyday surveillance" (Thompson & Warzel, 2020)

We need to ask over and over again, just because we can, should we? We might want this data but do we really need it? Are there any less intrusive and more secure ways of achieving the same purpose?

Accountability & Trust

Public and private entities must be transparent about the data being gathered, how they are processed and how the models guide public health and access to resource decisions; how long the data will be retained; and whether the entity envisages any negative outcomes and the decisions made regarding that trade-off. In times of panic, trust becomes even more important. Trust is what we need most right now. Trust in our officials, in our agencies, in our employers. If the public starts to think that these entities are trying to gain more power and do not have the public's interest in heart, they might stop following the guidelines coming from public health officials, like physical distancing, or avoiding unnecessary travel or following certain disinfection methods.

To that effect, we also need to keep the entities collecting the data accountable for the measures being taken, whether it is public, private or a combination of both. If necessary "trusted intermediaries" can be created from interdisciplinary backgrounds that could be the guardians of these dataset for the duration of time outlined for an initiative.

In its statement on March 19, 2020 European Data Protection Board has adopted that in principle, location data can only be used by the operator when made anonymous or with the consent of individuals. Although the statement suggests that Art. 15 of the e-Privacy Directive enables Member States to introduce legislative measures to safeguard public security, such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society. Moreover, it is subject to the judicial control of the European Court of Justice and the European Court of Human Rights (EDPB, 2020).

The interim guidance from World Health Organization (WHO) on Global surveillance for COVID-19 caused by human infection with COVID-19 virus states that public health surveillance is the continuous, systematic collection, analysis and interpretation of health-related data needed for the planning, implementation, and evaluation of public health practice. It says that the national authorities may use either case-based reporting or aggregate reporting (which is defined as "At national level: Weekly number of new confirmed cases; Weekly number of new confirmed case deaths from COVID-19; Weekly number of new confirmed cases hospitalized due to COVID-19 disease; Weekly number of confirmed cases discharged, etc…). WHO guidance does not require mass location surveillance or tracking of populations. They would like to keep their data transparent to help contain the pandemic and keep the trust the world population bestows on them untouched — for they know that they need that trust to succeed against this and future pandemics (WHO, 2020).

Respect for Data Rights & Privacy

Rich and accurate data makes our models more accurate, and in this case, it helps our decisions to fight the pandemic. However, as reminded us by Frank La Rue, UN Human Rights Council Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, at both the international and regional levels, privacy is unequivocally recognized as a fundamental human right. The right to privacy is enshrined by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (ICCPR, art. 17), the Convention on the Rights of the Child (art. 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14). At the regional level, the right to privacy is protected by the European Convention on Human Rights (art. 8) and the American Convention on Human Rights (art. 11). State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State (UN, 2013)

Invasion of privacy deters our free speech and association, and disparately impacts minorities. The Special Rapporteur also urges Governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity, in accordance with international human rights standards, and what measures have been taken to protect against abuse. He further reminds that in developing and deploying new technologies and communications tools in specific ways, corporate actors might take measures that facilitate State surveillance of communications. In its simplest manifestation, this collaboration takes the form of decisions on how corporate actors collect and process information, which allows them to become massive repositories of personal information that are then accessible to States upon demand.

Describing location data as anonymous is "a completely false claim" that has been debunked in multiple studies, Paul Ohm, a law professor and privacy researcher at the Georgetown University Law Center, says "Really precise, longitudinal geo-location information is absolutely impossible to anonymize" (Thompson & Warzel, 2020)

In two recent studies, researches underlined how difficult it is for any data set to meet that standard of being truly, robustly anonymous — given how the risk of re-identification demonstrably steps up with even just a few attributes available. One study was from Imperial College London and Université Catholique de Louvain where researchers have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes (Rocher & de Montjoye, 2019). In another study, which Imperial College's Yves-Alexandre de Montjoye co-authored, that investigated the privacy erosion of smartphone location data, researchers were able to uniquely identify 95% of the individuals in a data set with just four spatio-temporal points (de Montjoye, Hidalgo, Verleysen, *et al, 2013)*.

We need to remember that even though US and many other countries massively lack digital privacy protection regulation, privacy is a human right and thus be respected as such. The last thing we want is come out the other end of this pandemic where our freedoms and democracy is in danger.

Prevention of Harm & Bias

If you have been involved in any discussion of bias in algorithms, you would know how serious the consequences can be of bias embedded in these systems. Data is created by humans, of humans and for humans…and in that same vein it is humans that make decisions on what methods to use to collect data, how to process it & use their results and what to do with that data after public health emergency is over. So, it is within the ability of humans to prevent harm. Anyone involved in development and deployment of the surveillance technology, as well as anyone involved in creating models for authorities will naturally make a number of assumptions and hit a number of limitations. We need to acknowledge that the assumptions and hypotheses come with the biases of their developers, they come with the 'perceptions' of the modelers and not necessarily the reality as we can never have 100% of the facts and factors that are in play. So, in these times where our assumptions and perceptions have such huge impact on people's lives, we need to keep these teams as diverse, interdisciplinary and transparent as possible so that we can challenge each other to ensure a better approach. If there was an acknowledged negative outcome in these models and it was decided to move on nevertheless, those trade-offs decisions must be transparent. The people who make decisions on these models and their predictions, as well as the public who are being impacted and whose data is being used, must also be fully aware of the assumptions and any shortcomings.

In a recent statement on COVID-19 and ethical considerations, UNESCO has acknowledged that vulnerable individuals become even more vulnerable in times of pandemic. It is particularly important to take note of vulnerability related to poverty, discrimination, gender, illness, loss of autonomy or functionality, elder age, disability, ethnicity, incarceration (prisoners), undocumented migration, and the status of refugees and stateless persons (UNESCO, 2020). We have already seen some racist remarks regarding the origins and spread of coronavirus. The surveillance and containment efforts should not be driven by bias based on nationality, ethnicity or religion. We must ensure that whatever technological surveillance measure is being used (with a defined purpose, scope and duration), it also needs to ensure that the data and decisions are not biased, and that special precautions are taken to prevent harm to individuals.

Data collected should not be used to make decisions that would limit certain groups' access to resources — not during the pandemic and certainly not later. In 2018, the Supreme Court decided in Carpenter v. United States that when the police want to track a suspect's whereabouts at every moment over weeks or months in the past, the Constitution requires them to persuade a judge to issue a warrant based on probable cause (US Supreme Court, 2018). Once the case or challenge to use the data in the first place is met, the data should not be used further for other purposes. For example, data should not be provided to insurance companies in case they might decide not to provide coverage to individuals who have tested positive during the pandemic.

Following on that same note, the data should not be shared further with any agencies and/or companies that have no health involvement. After a pandemic, under the threat of a 'national security', the massive amounts of private data collected should not then flow into the databases of the public agencies like ICE or NSA, or their private partners like Palantir or Clearview.

Any action taken using the data analysis should not allow for a way to identify or de-anonymize any individual, business or area. The data should not provide a way for people to stigmatize the identified individuals, businesses or neighborhoods etc. that would have both social and economic impact on them. As suggested by the "Joint civil society statement (2020): States use of digital surveillance technologies to fight pandemic must respect human rights" signed by more than 100 privacy and human rights organizations, 'any use of digital surveillance technologies in responding to COVID-19, including big data and artificial intelligence systems, must address the risk that these tools will facilitate discrimination and other rights abuses against racial minorities, people living in poverty, and other marginalized populations, whose needs and lived realities may be obscured or misrepresented in large datasets."

The data collected should also not be used for disinformation purposes. We all know that there will always be those who will try to use data for their own personal or policy purposes and will not shy away from using disinformation or intentional misinterpretation.

Neither should they have disparate effect on the groups disadvantaged backgrounds, or geographical locations with poorer infrastructure. When rolling out initiatives that should be for 'public benefit' we should ask the question of who is not in the room. We should remember that if a technology requires the use of a smartphone with GPS, some vulnerable populations might not always have such devices available like the elderly, homeless and people living in low-income countries who are at high risk of infection and negative health outcomes. Ensuring that technology that works for all will be an important piece to mitigating the spread effectively.

CONCLUSION

One of the biggest datasets of the world is being created during the pandemic and it will make the powerful even more powerful. We need to side with ethics, morality and a sense of community. Exigent circumstances must not lead us down the road of trading our ethics for techniques and technologies that will impact our democracy under the guise of 'public health'. Yes, we need to stop the spread of this pandemic and make every effort to help save lives. Absolutely no question about it. However, this should not stop us from requiring the best from our governments, companies, communities.

REFERENCES

Amnesty International. (2020, April). *COVID-19, surveillance and the threat to your rights.* Retrieved from https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/

Chrysaidos, N. (2020, March). *Iranian Coronavirus app collecting sensitive information.* Retrieved from https://blog.avast.com/iranian-coronavirus-app-collecting-sensitive-information-avast

Cimpanu, C. (2020, March). *Spying concerns raised over Iran's official COVID-19 detection app.* Retrieved from https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/

de Montjoye, Y-A., Hidalgo, C., Verleysen, M., & Blondel, V. (2013, February). *Unique in the Crowd: The privacy bounds of human mobility. Sci Rep.*, 3, 1376. https://doi.org/10.1038/srep01376

EDPB - European Data Protection Board (2020, March). *Statement on the processing of personal data in the context of the COVID-19 outbreak.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Fouquet, H., & Torsoli, A. (2020, April). *Palantir in Talks with Germany, France for Virus-Fighting Tool.* Retrieved from https://www.bloomberg.com/news/articles/2020-04-01/palantir-in-talks-with-germany-france-for-virus-fighting-tool

Fussell, S. (2020, March). *How Surveillance Could Save Lives Amid a Public Health Crisis.* Retrieved from https://www.wired.com/story/surveillance-save-lives-amid-public-health-crisis/

Hao, K. (2020, March). *Coronavirus is forcing a trade-off between privacy and public health.* Retrieved from https://www.technologyreview.com/2020/03/24/950361/coronavirus-is-forcing-a-trade-off-between-privacy-and-public-health/

Hatmaker, T. (2019, August). *Secretive Tech Company Palantir Doubles Down on Its ICE Contracts.* Retrieved from https://www.thedailybeast.com/palantir-secretive-tech-company-doubles-down-on-its-ice-contracts

Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights. (2020, April). Retrieved from https://www.amnestyusa.org/wp-content/uploads/2020/04/FULL-STATEMENT.pdf

Lawmaker Says Iran Behind Bogus Messaging Apps, Banned by Google. (2019, May). Retrieved from https://en.radiofarda.com/a/lawmaker-says-iran-behind-bogus-messaging-apps-banned-by-google/29924990.html

Lubell, M. (2020, April). *Israel's top court says government must legislate COVID-19 phone-tracking.* Retrieved from https://www.reuters.com/article/us-health-coronavirus-israel-monitoring/israels-top-court-says-government-must-legislate-covid-19-phone-tracking-idUSKCN2280RN

Martin, A. (2020, March*). Coronavirus: Government using mobile location data to tackle outbreak.* Retrieved from https://news.sky.com/story/coronavirus-government-using-mobile-location-data-to-tackle-outbreak-11960050

Max, K. S. (2020, March). *South Korea is watching quarantined citizens with a smartphone app.* Retrieved from https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/

Mozur, P. (2020, March). *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags.* Retrieved from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Newton, C. (2020, March). *How Location data could play a role in managing the coronavirus crisis.* Retrieved from https://www.theverge.com/interface/2020/3/25/21192629/coronavirus-surveillance-location-data-taiwan-israel-us-google

Ongweso, E., Jr. (2020, January). *Palantir's CEO Finally Admits to Helping ICE Deport Undocumented Immigrants.* Retrieved from https://www.vice.com/en_us/article/pkeg99/palantirs-ceo-finally-admits-to-helping-ice-deport-undocumented-immigrants

Polonetsky, J. (2020, March). *Silicon Valley, Follow, Don't Lead.* Retrieved from https://www.linkedin.com/pulse/silicon-valley-follow-dont-lead-jules-polonetsky/

Privacy Act of 1974. (n.d). Retrieved from https://www.law.cornell.edu/uscode/text/5/552a

Renieris, E. (2020, March). *When Privacy Meets a Pandemic.* Retrieved from https://onezero.medium.com/when-privacy-meets-pandemic-fbf9154f80b3

Ringrose, K. (2020, March). *Privacy and Pandemics: A Thoughtful Discussion.* Retrieved from https://fpf.org/2020/03/27/privacy-and-pandemics-a-thoughtful-discussion/

Rocher, H., & de Montjoye Y. (2019, June). *Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun.*, 10, 3069. Retrieved from https://doi.org/10.1038/s41467-019-10933-3

Romm, T., Dwoskin, E., & Timberg, C. (2020, March). *U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus.* Retrieved from https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/

Saiidi, U. (2020, March). *Hong Kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine*. Retrieved from https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html

The Attorney Generals' Guidelines for Domestic FBI Operations: Guidance Implementing Federal Statutes relevant in the Information Sharing Environment (ISE). (n.d.). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/implementation

The 9/11 Commission Report. (n.d.). Retrieved from https://www.9-11commission.gov/report/911Report.pdf

Thompson, S. A., & Warzel, C. (2019, December). *Twelve Million Phones, One Dataset, Zero Privacy.* Retrieved from https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

UN – United Nations General Assembly. (2013, April). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue.* Retrieved from https://dig.watch/sites/default/files/A.HRC_.23.40_EN%25282%2529.pdf

UNESCO. (2020, April). *Statement on COVID-19: Ethical Considerations from a Global Perspective.* Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000373115/PDF/373115eng.pdf.multi

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. (n.d.). Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3162

US Supreme Court. (2018, June). *Carpenter v. United States.* Retrieved from https://supreme.justia.com/cases/federal/us/585/16-402/

USA Freedom Act of 2015. (n.d.). Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/2048/text

WHO – World Health Organization. (2020, March). *Global surveillance for COVID-19 caused by human infection with COVID-19 virus: Interim guidance*. Retrieved from https://www.who.int/docs/default-source/coronaviruse/global-surveillance-for-covid-v-19-final200321-rev.pdf