COVID-19 and the Rise of Participatory SIGINT: An Examination of the Rise in Government Surveillance Through Mobile Applications

Rose Bernard, MA, Gemma Bowsher, MBBS, MA, and Richard Sullivan, MBBS, FRCS, PhD

The COVID-19 pandemic has triggered a significant growth in government surveillance techniques globally, primarily through the use of cell phone applications. However, although these applications can have actionable effects on public health efforts to control pandemics, the participatory or voluntary nature of these measures is obscuring the relationship between health information and traditional government surveillance techniques, potentially preventing effective oversight. Public health measures have traditionally been resistant to the integration of government-led intelligence techniques, such as signals intelligence (SIGINT), because of ethical and legal issues arising from the nature of surveillance techniques.

We explore this rise of participatory SIGINT and its nature as an extension of biosurveillance through 3 drivers: the rise of surveillance capitalism, the exploitation of a public health crisis to obscure state of exception politics with a moral imperative, and the historically enduring nature of emergency-implemented surveillance measures.

We conclude that although mobile applications may indeed be useful in containing pandemics, they should be subject to similar oversight and regulation as other government intelligence collection techniques. (*Am J Public Health.* 2020;110:1780–1785. https://doi.org/10.2105/AJPH.2020.305912)

The COVID-19 pandemic has triggered a significant growth in government surveillance and monitoring techniques across the globe, largely through the use of cell phone applications and other smart device technologies.[1] Official government and media narratives have not presented these technologies as an extension of surveillance but rather as a transaction, which requires that individuals surrender data in exchange for the return of civil liberties after emergence from quarantine, or for the promise of an as yet unarticulated "safer" future. The underpinning rationale for these measures has been "the science," which governments have repeatedly presented as an apolitical regime naturally determining credible governance.[2]

Data collection falls under the definition of signals intelligence (SIGINT)—an intelligence collection technique that governs data collected from electronic or communications devices—or foreign instrumentation data.[3] In this practice there are 2 specific types of collection, "signals external," which deals with collecting the signal itself, its strength, frequency, and network traffic, and "signals internal," which deals with the message data.[4] Such collection has traditionally been associated with nation-state governments or government agencies and thus covert collection; however, a "democratization of SIGINT" has made these capabilities increasingly available for commercial purposes.[4]

In a public health context, the use of SIGINT and other unique intelligence tools has become increasingly integral to epidemic and pandemic preparedness and response, even if not overtly referred to in these terms, as national security doctrines expanded to include the pandemic threat.[5] Of all these intelligence methods, SIGINT is perhaps the most controversial: although it could be used in contact tracing, tracking adherence to quarantine, tracking health data from smartphones and connected devices, and tracking purchase data for location or prescription needs, there are significant legal, ethical, and normative barriers to its use.

Furthermore, the COVID-19 pandemic has occurred during an unprecedented period of technological integration into daily life. This has brought its own transactional data market, with individuals regularly trading personal data for access to services or products. Governments have exploited the normality of this transactional relationship with commercial technology during a pandemic-precipitated state of exception to introduce a new form of SIGINT. We frame this concept as "participatory SIGINT," because rather than harvesting data from passive surveillance participants, people participate in their own surveillance by readily surrendering personal data either directly through direct government-sanctioned or -sponsored technology or indirectly through trusted third parties. The participatory nature of this new SIGINT mechanism effectively allows the avoidance of normative, legal, and ethical barriers associated with traditional security sector SIGINT. In these discourses of necessity driving personal self-management through technology, the prominence of science as a legitimizing currency mediating extractive state–individual relations is made apparent.

ABOUT THE AUTHORS

All authors are with the Conflict and Health Research Group, Kings College London, London, UK.

Correspondence should be sent to Rose Bernard, Comprehensive Cancer Centre, Guy's Campus, Great Maze Pond, London, SE1 9RT, United Kingdom (e-mail: rose.bernard@kcl.ac.uk). Reprints can be ordered at http://www.ajph.org by clicking the "Reprints" link.

This article was accepted August 3, 2020.

https://doi.org/10.2105/AJPH.2020.305912

COVID-19 AND SIGINT USE

SIGINT is traditionally defined as intelligence deriving from communications and electronics data. This can include, but is not limited to, call, message, and e-mail contents and metadata, location data, purchases made using connected devices, health information recorded or collected by mobile applications, and information from connected devices such as smart watches and fitness trackers. It includes data gathered both at an individual level and, more controversially, at a bulk level from telecommunication or technology companies.[6] Traditionally, SIGINT has been considered a capability limited to security sectors of nation-states because of high operating costs, sensitivity of access, and costs connected with associated analysis. Crucially, SIGINT is governed by legal and regulatory frameworks.

A substantial number of traditional SIGINT techniques are being used in the management of the COVID-19 pandemic. There are currently 4 broad categories of data collection being used for this purpose:

1. Anonymized bulk data collection and telecommunications companies' provision of location data to governments: for example, the United States, the European Union, Canada, and South Korea are working with telecommunications companies to use telecoms data to track general compliance with social-distancing measures or to identify large groupings of individuals.[7,8]
2. Geofencing: countries have used geofencing data to implement and enforce mandatory quarantine. Taiwan and South Korean have implemented geofencing via cell phone data—a technique that alerts authorities when quarantined individuals leave their primary place of quarantine.[9]
3. Cell phone applications to support quarantine measures: some governments are using an application to achieve geofencing measures—for example, in Singapore quarantined individuals must click on links in text messages sent by health officials that sends location data back and can be used to track whether individuals have left their place of quarantine.[10]
4. Cell phone applications to support track and trace measures: many countries are developing cell phone applications to conduct and enhance contact tracing. For example, countries, such as South Korea, India, Hong Kong, Romania, Slovakia, and Poland, as well as some regions of Spain are using similar apps. Both the European Union and the United Kingdom are developing apps to track users; these apps determine proximity to other app users, and, if users come into contact with an individual who subsequently tests positive, they would be required to quarantine for a predetermined period of time.[11] This has been most evident in China, where the HealthCode apps work on user input and government-provided information, including health symptoms, test results, and location data to provide individuals with a red, orange, or green code that restricts movement accordingly.[12]

Although countries are implementing these techniques in different ways, globally there is an upward trend in the use of such surveillance measures. As of July 3, 2020, the privacy tracking site Top10VPN found that contact-tracing applications were being used in 28 countries, with alternative digital tracing measures used in 35 different countries and 47 applications emerging specifically to manage contact-tracing and quarantine measures of COVID-19 available globally.[13]

The majority of these applications are not, at least overtly, mandatory. Although anonymized bulk data collection of location and geofencing techniques and applications have been used to mandatorily enforce quarantine, cell phone applications intended to supplement track and trace are perceived as voluntary. Both the European Union and the United Kingdom have claimed that their applications will be voluntary; however, although participation may be overtly perceived as voluntary, nonadherence may have detrimental effects on individual freedoms. In China, for example, although the application remains technically voluntary, it is necessary for travel and entrance into most shops and restaurants, and building managers require it to rent an apartment. Nevertheless, the framing of these measures as voluntary participation marks a departure from traditional SIGINT while retaining the key features of large-scale personal data collection for surveillance purposes.

SIGINT and associated techniques, such as government agencies' bulk data collection, face a normative barrier to use that largely arose from the 2013 revelation of a mass data collection program the United States ran with the assistance of the United Kingdom.[14] Despite the difference in collection techniques and targeting between bulk data collection—or signals external—and the use of mobile applications to track and trace data that could include access to signals internal, the public perception of such techniques remains intertwined as a result of their association with government use. This, combined with subsequent reports on the commercialization of surveillance technology associated with SIGINT led to a public backlash against the use of government mass data collection and provoked a shift in public attitudes toward government mass surveillance.[15]

In the health domain, SIGINT has remained controversial, and although phone-tracking data have been used in complex humanitarian emergencies, such as tracking the 2012 Haiti earthquake victims, data-collection techniques have not yet been used at scale in pandemics, and questions regarding their effectiveness and quality persist.[16] In the 2003 SARS (severe acute respiratory syndrome) epidemic and the 2015 MERS (Middle East respiratory syndrome) outbreak, some rudimentary and localized tracking systems were used. Examples include RFID (radio-frequency identification) locators to track visitors to hospitals in Singapore and cell phone data to track quarantined individuals in South Korea; however, these practices did not become widespread globally.[17] Similarly, in the 2014 to 2016 Ebola outbreak, although mHealth applications were used to deliver health communications and advice to individuals in affected countries, connectivity and lack of cell phone ownership in rural areas hindered the use of SIGINT as a tracking or quarantine measure.[18]

It therefore appears that in seeking to avoid the public perception and regulatory implications of bulk data collection and covert surveillance, governments have opted for the use of mobile apps, often framed as voluntary, marking a departure from the contentious data collection techniques of traditional SIGINT. Nevertheless, the differences in public communication of these new applications during this pandemic have not significantly altered the nature of data collection and the use of communications data for broadly defined surveillance purposes.

THE GROWTH OF PARTICIPATORY SIGINT

We define "participatory SIGINT" as intelligence derived from communication devices or electronic devices, which includes mobile devices and smart devices and may include messaging contents, geolocations, health data, and contacts, or any part thereof, and which the data originator (also known as the "data subject" under the GDPR) provides voluntarily to government authorities or commercial authorities as part of a government-affiliated program. This can take place through a Web site or a mobile application. Participation is typically voluntary, although extenuating circumstances may involve coerced volunteering. Two key features of these technologies is the role of individuals as semivoluntary participants engaging in self-managing practices through these mobile applications and the use of a public health imperative to override ongoing privacy objections by presenting participation as engagement in necessary response measures. In the context of the ongoing COVID-19 pandemic, we therefore consider the use of government-developed, -sanctioned, -controlled, or -coordinated applications used to enhance or take the place of track and trace schemes to be participatory SIGINT.

Although the track and trace applications are used ostensibly for locating contact data and the quarantine applications for enforcing periods of isolation, in the course of this they collect data associated with traditional SIGINT, including location data, contact data, and travel data. A study of the HealthCode apps used in China revealed that information collected using the apps could draw an alarmingly detailed picture of the average city dweller's life, including their GPS (Global Positioning System) location, stores at which they shopped, meals ordered, rides or transportation used, specific bicycles rented, and even friends messaged and associated detailed social plans.[17] In fact, of the 47 applications currently available, 24 contain Google and Facebook tracking, 11 have no privacy policy, 25 do not disclose the length of time that they hold the data for, and 28 have no publicly disclosed anonymity measures.[13]

Public criticism of the government-proposed apps has moved away from traditional questions relating to SIGINT processes—which largely concern proportionality legality and regulatory oversight—and into the realm of data protection and regulation, effectively transferring the question from why to how. Although some data protection regulations, in particular the European Union's General Data Protection Regulations (GDPR), require a specific need for organizations to collect specific data, the intrusive and sensitive nature of the data collected make it difficult to apply the regulations. One of the fundamental principles of the GDPR is that data participants must consent to the processing of their information and to do so must be informed of the full scope, features, usage, and storage of those data.[19]

In unequal power balances, such as the relationship between employee and employer, some guidance has questioned whether it is possible for employees to voluntarily consent to the gathering, processing, and transference of their personal data.[20] In the context of a pandemic during which governments are asking individuals to hand over personal data without a full understanding of the extent, scope, and duration of application, it is difficult to understand how data participants can be fully informed of what they are consenting to and whether the unequal government–citizen power balance in an exceptional political environment can constitute consent.

This novel form of participatory SIGINT used in a public health event requires that individuals participate in their own surveillance by providing nation-state intelligence capabilities with information and, in so doing, consent to bypassing traditional state barriers and normative frameworks. In this definition, the use of the term "participatory" departs somewhat from its use in other settings such as "participatory governance," in which the emphasis is on diminishing gulfs between government and community actors as a mode of empowerment and democratization. In our use it reflects a contemporary mode of engaging individuals in government and commercial initiatives whereby voluntary or semivoluntary subscription (often via the use of mobile applications or online technologies) is used as a means of garnering collective public participation in programs employing broad-based SIGINT processes, often with indeterminate limits on collection and data use.

We have identified 3 drivers in the growth of participatory SIGINT during the COVID-19 pandemic: (1) the Trojan horse of surveillance capitalism, (2) the politics of exception as moral imperative, and (3) the endurance of emergency-implemented surveillance measures.

Trojan Horse

Surveillance capitalism is the commodification of our personal data by companies that provide "free" services to collect and generate our behavioral data to sell in "behavioral futures markets," a concept coined and explored by author Shoshana Zuboff.[21] The prevalence of these practices is in part attributable to these services' transactional nature—which, despite the heavy balance in favor of the companies, generates the sense that individuals are deriving a desirable and worthwhile benefit via a service of convenience. Surveillance capitalism is a new phase in "dataveillance," a term that reflects the collection of personal data and its aggregation into a surveillance model but wherein, by framing it as a transaction, the user maintains the illusion of participation by choice.[22] This practice has become increasingly pervasive and intertwined with the growth of our reliance on technology, to the extent that the encroachment of digital devices collecting personal data has been compared with the process of colonialism: whereas historical practices of colonialism targeted physical

territories and countries, contemporary data colonialism targets our personal information for profit, and "human experience, potentially every layer and aspect of it, is becoming the target of profitable extraction."[23(px)]

Despite ongoing revelations about the treatment of our personal data, or perhaps because of the ubiquity of them, this attitude toward companies' use of personal data continues to persist. A watershed moment for public privacy—the news in 2018 that UK company Cambridge Analytica had harvested the data of up to 87 million Facebook users and used it for political campaigning—resulted in few lasting consequences: Facebook was fined the equivalent of $663 000 by the UK Information Commissioner's Office and $5 billion by the US courts (a low amount for a company whose turnover for 2018 alone was $56 billion). Although Facebook's publicly traded stock value fell by 24% in the week following the report, it had recovered less than 2 months later. Despite growth in calls for regulation, little has changed in Facebook's day-to-day regulatory practices. The illusion of a transaction we recognize—personal data for access to services—grants the user a false sense of risk mitigation and control.[24]

Thus, by framing the SIGINT associated with managing quarantine and contact tracing as an app, governments are packaging traditional surveillance capacities as a transaction associated with surveillance capitalism—and therefore associated with risks that the user recognizes and is relatively willing to accept. This practice has driven a critical conceptual shift whereby the framing of this method in the terms of surveillance capitalism instead of a SIGINT method draws focus to the norms and methods of data protection, rather than the regulatory oversight of intelligence capabilities. Consequently, further government use of these data has gone relatively unexamined. Although many governments promise anonymity, this is often flawed in practice: a study carried out on anonymized data found that nearly all people can be identified from just 15 separate characteristics.[25]

Additionally, although users may choose to provide information based on current and specific need, the absence of a regulatory framework means that the ability to enforce this consent is limited in the longer term. For example, on March 12 the UK Information Commissioner's Office asserted, "Public bodies may require additional collection and sharing of personal data to protect against serious threats to public health"—a statement vague enough to cover a wide range of current and future possibilities.[26]

Politics of Exception

A state of exception can be conceptualized as an emergency regime in which a government can extend the boundaries of sovereignty by increasing its power during times of supposed crisis or as a space that allows a state to operate without a legal framework.[27] The current pandemic has been overwhelmingly securitized by Western governments, who have framed it as a war or a state of war by employing the language of exception to create a state of emergency requiring recourse to extensive powers while also using the nature of the public health crisis as a moral imperative to justify that creation.[28] This war-like rhetoric of the "invisible enemy" has formulated an "us" against "it" framing, whereby exceptional state measures normally subject to close public scrutiny have been legitimized under a doctrine of necessity, and the moral dimension of the "right" and "wrong" sides created in warfare has protecting this framing from criticism.

The character of war as the basis of a state of exception during a public health crisis has had the effect of increasing the legitimacy of military involvement during public health responses. In settings such as the United Kingdom and the United States, for example, military units have been deployed to support the COVID-19 response at the same time that their governments have received widespread criticism for failing to invest in or deliver timely and effective public health measures, such as contact tracing and widespread testing regimes.[29] This character of war has also meant that certain measures that would normally represent a failure of public health measures, such as nationwide quarantines, are instead seen as a first line of defense that secondary public health measures do not necessarily effectively support.

The convergence of security narratives with discourses of scientific necessity has been a key step in generating the moral imperative that has mediated individual engagement with surveillance technologies. The UK secretary of state for health, Matt Hancock, publicly stated that downloading the prospective UK government contract tracing app constituted a "civic duty" crucial to "getting our liberty back."[30] In this framing, participation in the contribution of SIGINT data is presented as a necessary sacrifice of civil liberties and as part of individual participation in a national effort during a science-led war.

Emergency Surveillance Measures

States of exception, and measures introduced to manage them, are intended to be temporary; however, history has demonstrated that surveillance measures introduced during crises are rarely later rolled back. This is particularly evident in the sweeping intelligence reforms the United States introduced under the Patriot Act following the 2001 terrorist attacks in New York, which granted unprecedented surveillance and SIGINT powers to law enforcement and intelligence agencies. These measures were supposed to expire in 2005, but the majority of them have been renewed regularly in varying form, regardless of the sitting president's party affiliation. The erosion of civil liberties tends to aggregate over time, with each new iteration expanding in scope.[31]

Accordingly, oversight for the use of participatory SIGINT, including need-based temporally restricted permissions, is crucial. By using mobile apps in health crises operating under data protection rather than intelligence regulation, we risk normalizing this surrendering of personal data both during and outside emergencies. Although many may consider the use of apps and the relinquishing of personal data to be proportionate and legal in the case of this pandemic, this is unlikely to automatically be the case in all future permutations of these programs.

CONCLUSIONS

We do not intend to present a general opposition to the use of mobile technologies in public health crises: there is evidence that their use can present a significant contribution to the opening of

quarantine, the management of quarantine stages, or the initial stages of infection within countries. Indeed, there is some evidence that given the speed of transmission associated with COVID-19, digital contact tracing may be a highly effective tool for disease control.[32] However, we argue that the use of these applications should be overtly recognized as an extension of state intelligence and surveillance capacity and data collection. Clarity in methods, usage, and regulation should be paramount in the rollout of these applications, and the "soft" coercion of individuals into surrendering personal data for these purposes should be recognized as an ethically challenging domain. Participants should not be coerced into consenting to having their data collected without being fully aware of the nature and scope of the processing and the programs and other applications that they access or with which they share data.

We also call for transparency around the objectives of these apps: if they are deemed necessary for use in this pandemic then they should be time limited to the duration of this pandemic and subject to regular and transparent reviews. At all times during such health emergencies, processes meant to guide personal conduct or to collect personal data should be made visible at an individual level. Merely claiming that an application is voluntary does not mean that its processes, purposes, and functions are visible or excuse the obfuscation of its internal practices in the short or long term.

We also contest the supposed difference between coercive data extraction and voluntary provision of personal information via these applications. Some have claimed that the voluntary provision of data is a path to the avoidance of potentially coercive surveillance; however, although the process of submission may vary, the nature of the data collected and their processing, analysis, and dissemination remain in keeping with SIGINT practices.[32] In obscuring the similarities between these processes, both methods become more opaque and the collection of neither form of data should be made a condition of public health or the possession of civil liberties.

In particular, health data should be treated with more caution, not less. History has shown us repeatedly that health and population metrics have been used as tools of discrimination, including the denial of health insurance and thus the denial of health care to disenfranchised populations in the United States and the Chinese adoption of biosurveillance in its suppression of the Uighur population in Xinjiang province.[33]

It is imperative, therefore, that, whether participatory or not, collection of these data should be governed by legislation similar to other national intelligence capacities, recognizing the highly sensitive nature of these data and subjecting them to high levels of regulatory oversight. In addition, such measures should be used only within a national security preparedness and response framework to specific pandemics, not as a part of normative public health demand–led advisory functions. As a SIGINT capacity, apps should not be automatically deployed in broadly defined health contexts, whether infectious disease outbreaks or other national crises. Instead each situation should be required to reach the proportionality and legality aspects of all SIGINT uses to avoid the unfettered penetration of extractive surveillance technologies in our daily lives both during and beyond the COVID-19 pandemic. AJPH

CONTRIBUTORS

All authors contributed equally to the research and drafting of this article.

ACKNOWLEDGMENTS

This article was funded by the UK Research and Innovation Global Challenges Research Fund (research for health in conflict ES/P010962/1).

CONFLICTS OF INTEREST

The authors have no potential or actual conflicts of interest to disclose.

HUMAN PARTICIPANT PROTECTION

No protocol approval was necessary because no human participants were involved in this study.

REFERENCES

1. Gershgorn D. We mapped how the coronavirus is driving new surveillance programs around the world. 2020. Available at: https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9. Accessed May 5, 2020.

2. King-Hill S, Powell M. Coronavirus: what does it mean when the government says it is "following the science"? 2020. Available at: https://theconversation.com/coronavirus-what-does-it-mean-when-the-government-says-it-is-following-the-science-137109. Accessed July 6, 2020.

3. Joint Chiefs of Staff. Department of Defense: Dictionary of Military and Associated Terms. 2016. Available at: https://fas.org/irp/doddir/dod/jp1_02.pdf. Accessed September 10, 2020.

4. Weinbaum C, Berner S, McClintock B. SIGINT for anyone: the growing availability of signals intelligence in the public domain. 2017. Available at: https://www.rand.org/pubs/perspectives/PE273.html. Accessed July 3, 2020.

5. Bernard R, Bowsher G, Milner C, Boyle P, Patel P, Sullivan R. Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *J Public Health (Berl.)*. 2018;26(5):509–514. https://doi.org/10.1007/s10389-018-0899-3

6. National Security Agency Central Security Service. Signals intelligence. 2020. Available at: https://www.nsa.gov/what-we-do/signals-intelligence. Accessed May 5, 2020.

7. Scott M, Cerulus L, Kayali L. Commission tells carriers to hand over mobile data in coronavirus fight. 2020. Available at: https://www.politico.eu/article/European-commission-mobile-phone-data-Thierry-Breton-coronavirus-covid19. Accessed May 5, 2020.

8. Tau B. Government tracking how people move around in coronavirus pandemic. 2020. Available at: https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-115853932020. Accessed May 5, 2020.

9. Ghaffary S. What the US can learn from other countries using phones to track COVID-19. 2020. Available at: https://www.vox.com/recode/2020/4/18/21224178/covid-19-tech-tracking-phones-china-Singapore-Taiwan-Korea-google-apple-contact-tracing-digital. Accessed May 5, 2020.

10. Wetsman N. Google and Apple's COVID19 tracking system can't save lives all on its own. 2020. Available at: https://www.theverge.com/2020/4/15/21222161/apple-google-Bluetooth-contact-tracing-system-coronavirus-health. Accessed May 5, 2020.

11. Mancourt V. EU data regulator calls for pan-European COVID-19 app. 2020. Available at: https://www.politico.eu/article/coronavirus-Europe-data-regulator-calls-for-pan-european-covid-19-app. Accessed May 5, 2020.

12. Mozur P, Zhong R, Krolik A. In coronavirus fight, China gives citizens a color code, with red flags. 2020. Available at: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Accessed May 5, 2020.

13. TOP10VPN. COVID-19 digital rights tracker. 2020. Available at: https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker. Accessed May 5, 2020.

14. Hopkins N. UK gathering secret intelligence via covert NSA operation. 2013. Available at: https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism. Accessed May 5, 2020.

15. Lyon D. *Surveillance After Snowden*. Cambridge, UK: Polity Press; 2015.

16. Wilson J. The use of intelligence to determine attribution of the 2010 Haiti cholera disaster. *Intell Natl Secur*. 2018;33(6):866–874. https://doi.org/10.1080/02684527.2018.1464430

17. Cha S. Mapping coronavirus: South Koreans turn to online tracking as cases surge. 2020. Available at: https://www.uk.reuters.com/article/us-china-health-South Korea-maps/mapping-coronavirus-south-koreans-turn-to-online-tracking-as-cases-surge-idUKKCN20I0HG. Accessed May 5, 2020.

18. Bernard R, Sullivan R. The use of HUMINT in epidemics: a practical assessment. *Intell Natl Secur*. 2020;35(4):493–501. https://doi.org/10.1080/02684527.2020.1750137

19. Schulz M, Hennis-Plasschaert JA. Regulations. *Official Journal of the European*

Union. May 4, 2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Accessed July 3, 2020.

20. Jodka S. The GDPR covers employee/HR data and it's tricky, tricky (tricky) tricky: what HR needs to know. 2018. Available at: https://www.dickinson-wright.com/news-alerts/the-gdpr-covers-employee-hr-data-and-tricky. Accessed July 3, 2020.

21. Zuboff S. *The Age of Surveillance Capitalism*. London, UK: Profile Books; 2019.

22. Clarke R. Information technology and dataveillance. *Commun ACM*. 1988;31(5):498–512. https://doi.org/10.1145/42411.42413

23. Couldry N, Mejias U. *The Costs of Connection*. Palo Alto, CA: Stanford University Press; 2019. https://doi.org/10.1515/9781503609754

24. Wong J. The Cambridge Analytica scandal changed the world but—it didn't change Facebook. 2019. Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook. Accessed May 5, 2020.

25. Rocher L, Hendrickx J, de Montjoye Y. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun*. 2019;10(1):3069. https://doi.org/10.1038/s41467-019-10933-3

26. Information Commissioner's Office. Data protection and coronavirus. 2020. Available at: https://www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus. Accessed May 5, 2020.

27. Humphreys S. Legalizing lawlessness: on Giorgio Agamben's state of exception. *Eur J Int Law*. 2006;17(3):677–687. https://doi.org/10.1093/ejil/chl020

28. Sears N. The securitization of COVID-19: three political dilemmas. 2020. Available at: https://www.globalpolicyjournal.com/blog/25/03/2020/Securitization-covid-19-three-political-dilemmas. Accessed May 5, 2020.

29. Fall F. Coronavirus: how to avoid military responses becoming a double edged sword. 2020. Available at: https://theconversation.com/coronavirus-how-to-avoid-military-responses-becoming-double-edged-swords-135262. Accessed July 3, 2020.

30. Johnston J. Matt Hancock says public has a "duty" to download coronavirus contact tracing app. 2020. Available at: https://www.politicshome.com/news/article/matt-hancock-says-public-have-a-duty-to-download-coronavirus-contact-tracing-app. Accessed July 6, 2020.

31. McDonald S. We can't let the coronavirus lead to a 9/11-style erosion of civil liberties. 2020. Available at: https://www.theguardian.com/commentisfree/2020/mar/23/coronavirus-civil-liberties-authoritarian-measures. Accessed May 5, 2020.

32. Ferretti L, Wymant C, Kendall M, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*. 2020;368(6491):eabb6936. https://doi.org/10.1126/science.abb6936

33. Wee S. China uses DNA to track its people, with the help of American expertise. 2019. Available at: https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermofisher.html. Accessed May 5, 2020.