PUSHING THE LIMITS OF ACCOUNTABILITY: BIG-DATA ANALYTICS CONTAINING AND CONTROLLING COVID-19 IN SOUTH KOREA

Abstract

Purpose: The authors aim to illustrate how Big-data analytics pushed the limits of individuals' accountability as South Korea tried to control and contain Covid-19.

Design/methodology/approach: The authors draw upon Deleuzo-Guattarian framework elaborating how a surveillant assemblage was rhizomatically created and operated to monitor a segment of the population holding them accountable. Publicly available secondary data, such as press release from the government and media coverage, were used.

Findings: A COVID-19 Smart Management System and a Self-Quarantine Safety Protection App constituted a surveillance assemblage operating in a "state-form". This comprises the central and provincial governments agencies, local councils, policing systems, providers of telecommunication and financial services, and independent groups of people. This assemblage pushed the limit of accountability as individuals who tested positive or might bear possible future risks of the infection and transmission were held accountable for their locations and health conditions.

Practical implications: Policy makers may consider constructing this type of state-form for containing and controlling pandemics, such as Covid-19, while dealing with the issue of undermined privacy.

Social implications: The mass may consider to what extent individuals' personal information should be protected and how to hold the governments accountable for the legitimate use of such information.

Originality/value: While accountability studies have largely focused on formal organisations, we illustrated how a broader context of a state-form, harnessing Big-data analytics, pushes the limits of accountability.

Key words: Big-data analytics, accountability, privacy, surveillant assemblage, Covid-19, South Korea

1. Introduction

Illustrating how South Korea (Korea hereafter) has responded to the Covid-19, this paper explores how Big-data analytics (BDA) has pushed the limits of individuals' accountability. Recent studies have explored how BDA is enlisted in accountability mainly within commercial organisations (Arnaboldi et al., 2017; Andreassen, 2020). However, we know little about how BDA has shifted the practices of accountability in broader societal settings and push their limits. We illustrate this from a story of how individual Koreans were held accountable for containing and controlling the pandemic within their interconnected social settings.

To theorise this empirical finding, we draw on the notion of "societies of control" espoused by Gilles Deleuze and Felix Guattari who envisaged a regime of accountability beyond

organisational boundaries. This new regime makes population accountable for their health conditions as BDA enabled this mode of accountability to penetrate individuals' body. Simultaneously, this system collected and utilised individuals' location and biometric data such as body temperature, thereby pushing the limits of accountability (Messner, 2009).

This new system of accountability functions in a virtual space which Deleuze and Guattari (1987) labelled an "assemblage", and it operates based on actors' desire (Deleuze and Guattari, 1987; Haggerty and Ericson, 2000). In a pandemic situation, a government would desire to contain and control the disease, thereby demonstrating and enhancing its legitimacy and approval rate, while citizens would desire to maintain their health and safety. We examined how an individual citizen's body was held accountable to a surveillant assemblage, which pushed limits of accountability. Relying on the data collected from the public domains (See Appendix 1), such as government press releases and media coverage (both in English and Korean), we demonstrate how it occurred in Korea.

The remainder of the paper is structured as follows. Section 2 reviews the literature on BDA and accountability and elaborates on the theoretical perspective based on the ideas of Deleuze and Guattari. Section 3 illustrates how Korea handled the pandemic through a surveillant assemblage. Section 4 concludes the paper.

2. Theoretical framing

2.1 BDA, limits of accountability and privacy

Accountability, which is usually construed as "giving and demanding reasons for one's conduct" (Roberts and Scapens, 1985, p. 447), has often been seen as an organisational phenomenon although the organisation interacts with a wider societal context. While accountability research explored how such systems are constructed, justified, and maintained within organisational boundaries (e.g. O'Dwyer and Unerman, 2007), little is known about how it operates beyond these boundaries (cf. Alawattage et al., 2019). As BDA exploits information from multiple data-bases rather than from a single set of information, which is implicitly assumed within the social and environmental accounting literature (Leong and Hazelton, 2019), a new setting is created for giving and demanding reasons for one's conduct. So, we consulted the literature to understand how BDA is pushing the limits of accountability and then the related issue of privacy.

Big-data technologies have brought enormous changes to management and accountability. They shifted our reasoning from a deductive form to an abductive form (Arnaboldi et al., 2017), our decision-making modes from causality to correlation, and our analytical focus from samples to populations (Mayer-Schonberger and Cukier, 2013). Accounting researchers have examined how BDA has transformed accountability within organisations (Arnaboldi et al., 2017; Vasarhelyi et al., 2015). Some have studied how accountability systems harnessed Big-data technologies, including GPS and CCTV, to hold their employees accountable for their conduct (Moll and Yigitbasioglu, 2019). Such surveillance practices have become common in many commercial organisations as managers tend to mistrust employees (Fuch, 2011). Simultaneously, these practices have pushed the limits of accountability as individuals, who are labelled as "opaque selves" and "exposed selves" who cannot remember the minutiae of events in which they were involved and are unconscious of this accountability, respectively, are now held accountable to the BDA-enabled surveillant regime (Messner, 2009). Such a regime constructs accountable individual under "the condition of becoming a subject": those who are now aware of themselves being transparently monitored make themselves further subjectivized (Roberts, 2009, p. 959).

The surveillant regime has been observed at a societal level. Mayer-Schonberger and Cukier (2013) found that just like coloured young men living in a deprived area are more likely to be stopped and questioned by patrolling policemen on the streets due to higher likelihood of crime, middle-aged men with obesity and hypertension are charged by BDA higher premium for health insurance with an obligation to get regular medical check-ups. These two population categories are likely to comply with the terms and conditions of the insurance and directions of the policemen, respectively, due to their desire for survival and guilt caused by their biometric features, such as blood pressure and skin-colour. Now they are held accountable for possible future risks their body might bear through this surveillance. This practice is pushing the limits of individuals' accountability (Messner, 2009), while the inherent risks are being transferred to those individuals. Moreover, such surveillances carry privacy issues because it uses (or often misuses) personal information (Fuch, 2011).

As privacy is a social construct, its boundary depends on sensitivity of disclosed information perceived in a society (Davis, 2009). In a liberal society, individuals' right to privacy is taken for granted and highly valued (Fuch, 2011). Their personal information can only be used if they waive their right to privacy by voluntarily disclosing their information (i.e. via social media) or giving a third-party informed consent to its use (Mayer-Schonberger and Cukier, 2013). However, privacy right can be undermined by commercial organisations harnessing BDA (Moffitt and Vasarhelyi, 2013). These organisations exploit information on customers' credit-card transactions and/or their online behaviours for commercial purposes (Fuchs, 2011). This information might have been originally collected legitimately, but later they are shared (and/or even sold) and exploited often without the customers' knowledge (Mayer-Schonberger and Cukier, 2013). Nevertheless, in a pandemic situation, people now tend to become less sensitive to the privacy issues.

2.2 Assemblage: pushing the limits of accountability

Assemblage is understood as "a way of assembling or arranging" for an "ordering or arrangement" (Deleuze and Parnet, 2007, p. xiii). It comprises heterogenous materials, such as bodies, actions, and desires, which interrelate and alter one another like a rhizome. Deleuze and Guattari (1987) characterised a rhizomatic structure as non-central, non-hierarchical, open, and continuously moving network. The rhizomatic assemblage operates as a self-governing entity along with other heterogeneous materials and even with other assemblages, unlike in an orthodox state which is stratified as a form of governance within a "hierarchised aggregate". Deleuze and Guattari (1987) conceptualise this unorthodox form of governance as a "state-form", which assembles and arranges the heterogenous materials into a homogenised order.

An assemblage is organised in a territory, but it also de-territorialises and re-territorialises to form a governable order (Deleuze and Guattari, 1987). Deleuze and Guattari (1987) elaborated on this by illustrating how nomadic troops moved from "smooth" spaces to "striated" spaces. The striated spaces, such as a city enclosed by walls, are mappable, understandable, and thus governable by an established state. In contrast, smooth spaces, such as steppes, are anthropogeographically amorphous, non-formal and open. Nomadic troops living in smooth spaces continuously territorialise striated spaces, which are, in turn, de-territorialise enabling them to "establish, occupy, and extend" their smooth spaces (Deleuze, 1995, p. 33). In accounting research, these ideas were used to study how the creation and delivery of news is being de-territorialised from mainstream media, a striated space, and then re-territorialised in social media, a smooth space, wherein news is constantly assembled and arranged freely without hierarchy or centre (Carter and Whittle, 2018; Munro and Thanem, 2018). So, we understand

that an assemblage is ceaselessly moving, continuously territorialising, de-territorialising and re-territorialising spaces making them fluid and self-governing.

Deleuze and Guattari saw that assemblages operate in a wider regime of control, which they labelled as "societies of control" (Deleuze, 1992, pp. 3-4). This regime is "underpinned by continuous forms of free-floating control, which…are not restricted to particular sites of confinement" (Munro and Thanem, 2018, p. 72). The societies of control "spread out everywhere", creating "rhizomatic movements" (Deleuze and Parnet, 2007, p. ix, 67). These movements are fluid and open, where humans, artefacts, and institutions are inter-connected in a decentralised and non-hierarchical manner forming "a continuous network" (Deleuze, 1992, p. 6). Deleuze and Guattari (1987) argued that "desires are the basis of every society" (p. 219) and that it is desires that construct the rhizomatic assemblages and drive the rhizomatic movements of the assemblages in societies of control.

A rhizomatic assemblage was seen in our case study. Thanks to BDA, both structured and unstructured data generated and collected by various organisations and machines can be assembled and arranged to capture "who is infected at which locations" (Chang et al., 2020, p. 1). Consequently, those who tested positive and those who contacted them can be accountable for their locations and health conditions in respect of a possible future risk of Covid-19 infection and transmission, mostly without their knowledge.

3. The surveillant assemblage in Korea

On 19 January 2020, Korea's first case was confirmed for Covid-19, which was initially reported in Wuhan, China, in December 2019 (Lee and Lee, 2020). Consequently, the number of daily confirmed cases soon soared and reached its peak with 909 cases in Korea on 29 February 2020[i]. In response, Korea tried to contain and control it focusing on 3Ts: fast Testing (testing as quickly as possible), meticulous Tracing (tracing trajectories of those who have tested positive and those in contact with them) and appropriate Treating (treating those who tested positive) (MoHW, 2020c). For our analysis, we focus only on track and tracing technologies, namely, the COVID-19 Smart Management System and the Self-Quarantine Safety Protection App, which formed a surveillant assemblage. This surveillant assemblage was rhizomatically constructed and operated to hold those who tested positive and those in contact with them for likely risks their body might bear.

3.1. COVID-19 Smart Management System: enacting a State-form

From the first confirmed case, the Korean Center for Disease Control and Prevention[ii] (KCDC: an agency under the Ministry of Health and Welfare (MoHW)) conducted shoe-leather epidemiological investigations tracking and tracing the trajectories of those who tested positive for the previous 14 days by interviewing them and then publicising this information via its webpage (http://ncov.mohw.go.kr/en) (Lee and Lee, 2020). As the number of confirmed cases skyrocketed in February 2020, KCDC, the Ministry of Land, Infrastructure, and Transportation (MoLIT), the Ministry of Science and Information and Communication Technology (MoSI) agreed to develop a real-time automatic contact tracing system (MoLIT, 2020a). Consequently, the COVID-19 Smart Management System (the System hereafter) was introduced digitising the entire contact tracing process. This happened in a few weeks and piloted for ten days from 16 March 2020 (KHARN, 2020). The Smart City Data Hub technology, a type of BDA, expedited this development. The technology had already been developed since 2015 by 120 public and private institutions participating in an initiative of MoLIT for purposes of collecting and harnessing urban data on traffic, safety, and energy uses (KHARN, 2020). While Arnaboldi et al.

(2017) reported how metropolitan cities now collect and harness a wide range of urban data, such as "signals from diverse sources, geo-referenced social media data, mobile phone data, Wi-Fi data, traditional data and many others" to manage, control and predict activities within the cities (pp. 765-766), the System exploited such urban data to contain and control Covid-19. What we see here is the System territorialised networks of the government and private agencies in a rhizomatic rather than hierarchical manner, a state-form created in an emergency situation.

The fully-fledged System has been in place since 26 March 2020 for epidemiological investigations. Mr Park, a director at KCDC who oversaw the System operation stated that "the System has made contact tracing faster. It gives a lot of help in our response to contain Covid-19" (Policy Briefing, 2020). As the System was considered successful, MoLIT[iii] held a press conference (including foreign press) on 10 April 2020 to publicise this success. Answering questions from journalists, Mr Park elaborated:

> [The System] allows real-time process of large-scale urban data. Also, machine learning technologies are incorporated in the System…. The System collects personal information of the confirmed cases which are determined by the Health officials, epidemiological investigators…. The information used includes the location data from [three] telecommunications companies and credit card records [from 22 companies] (MoLIT, 2020b).

Mr Park's statement indicates that the System was enabled by BDA and formed a rhizomatic surveillant assemblage. Personal data previously collected and stored discretely by telecommunication companies and finance corporations were territorialised and then assembled and re-arranged into the System on a real-time basis. Considering that most Koreans use smart phones[iv], most economic transactions were processed without involving cash by debit or credit cards. These are tied to the owners' national identification number (Lee and Lee, 2020). So, this surveillant assemblage could monitor people's everyday trajectories.

When those who tested positive did not clearly remember where they went and whom they closely contacted (Messner (2009) would label them "opaque selves"), CCTV footages for the "previous fifteen days (the maximum incubation period of the virus)" were added by the Korea National Police Agency (the Police hereafter) to the System "to clarify missing links" (MoLIT, 2020b). Hence, the System territorialised the Police to reinforce the contact tracing. KCDC was then able to reconstruct in ten minutes the trajectories of those who tested positive in detail and cross-check others who contacted them (Lee and Lee, 2020). If a person who previously visited a certain place tested positive later, everyone in that place would be sent a text message advising them to be tested (Bicker, 2020). So, the System territorialised three telecommunication service providers, 22 debit/credit card companies, and the Police, rhizomatically assembling and arranging the surveillance information about the location of individuals' body which was previously stored discretely (Deleuze and Guattari, 1987; Haggerty and Ericson, 2000). Therefore, we regard the System as "the computer that tracks each person's position … [and]… singles out potential sick people and subjects at risk" (Deleuze, 1992, p. 7).

Once the location information was gathered, it was released to the public. An official for crisis communication at KCDC stated:

> We share with the public only places where there was close contact or infections could have spread - like where there are many people, where the patient was known to have not worn a mask (Kim, 2020).

This information initially released on MoHW's website was further disseminated in different forms by various parties. Local councils sent everyone within their territory the latest updates via text messages to lead them to avoid infection hotspots, compare their own trajectories with those publicised, and decide whether to be tested and/or self-quarantine. An example of this type of text message reads:

> 15th foreigner in Jongno-gu (a borough in Seoul) staying at the Somerset Palace Hotel in Seoul has tested positive. For more information, such as their path of movement, please visit our website (Kasulis, 2020).

Local councils sent this type of alert messages using a location-based technology, and thus as one moved from one borough to another via bus or subway, (s)he would receive the messages from different jurisdictions. Locational information of everyone's body was shared on a real-time basis through a mobile phone by telecommunications companies with local councils which have now been territorialised by the System. Hence, individuals became what Messner (2009) called "exposed selves" who were held accountable for their location not necessarily cognisant of this accountability. So, the System has pushed the limit of accountability of individuals due to possible future risks of infection and transmission that their bodies might bear.

Moreover, independent groups of people further processed the publicly available information to make it more user-friendly and disseminated it via websites and applications. A number of websites, such as http://coronamap.site[v] and https://corona-live.com/[vi] provided real-time exposure maps which disclosed the trajectories of the infected patients and hotspots on virtual maps in addition to visualising the official statistics of Covid-19 deaths and confirmed cases (Lee and Lee, 2020). In this regard, several mobile applications that had similar functions, such as "Corona 100m", were developed independently. Mr Bae, the developer of Corona 100 metre, stated:

> [This type of applications] allows people to see the date that a coronavirus patient was confirmed to have the disease, along with that patient's nationality, gender, age and where the patient visited. The person using the app can also see how close they are to coronavirus patients (Watson and Jeong, 2020).

As these websites and applications were developed independently of the government, the System has territorialised a smooth space of the general public, whose desire enabled the rhizomatic dissemination of the information.

Most Koreans found that the dissemination of the information was useful, but they were concerned about its excessive transparency because all personal data such as surname, age, residential suburb, travel routes of confirmed patients were disclosed (Song, 2020). The excessive transparency resulting in privacy violation was caused by revision of legislation in after MERS (Middle East Respiratory Syndrome) outbreak in 2015. Then 2931 people quarantined, of whom 186 tested positive (the second largest number after Saudi Arabia) and 39 died, and Koreans have developed their desire for health and safety at the expense of privacy and personal information. So, then government was accused by the mainstream media of withholding from the public the information about MERS patients (Kasulis, 2020). Consequently, the *Contagious Disease Prevention and Control Act* was revised in July 2015 to exceptionally override some provisions of the *Personal Information Protection Act,* which "in principle bans the collection, use, and disclosure of personal data without prior informed consent of the individual whose data are involved" (Park et al., 2020, p. 2129). Since this legal amendment, "location data collected from mobile devices, personal identification information, medical and prescription records,

immigration records, card transaction data … transit pass records for public transportation, and CCTV footage" were allowed to be legitimately gathered for a contagious disease prevention and control purpose (Park et al., 2020, p. 2129). In this context, current government highlighted transparency as a key principle in response to Covid-19 (MoHW, 2020c) and the System territorialised these types of data.

At an early stage of pandemic, foreign media emphasised Koreans' preference of transparency over privacy by interviewing the general public:

> It's good for people to know if there are infected people visiting the same places that they might go to (a male in his 20s) (Kasulis, 2020).
>
> I think we should provide that amount of information. When confirmed patients occur, both my friends and I go online to check their routes (a male in his 20s).
>
> It is a violation of privacy, but it is necessary (a female in her 60s) (Bicker, 2020).

So, the Koreans' desire for health and safety outweighed their privacy concern caused by disseminated personal information. They also valued transparency higher than privacy to contain and control Covid-19. Therefore, transparency deemed a "vital social practice – an exercise of care in relation to self and others" (Roberts, 2009, p. 969) at the early stage of the pandemic.

Nevertheless, as the public concern about privacy violation grew, the law was re-revised in September 2020 to better protect personal information: information irrelevant to an epidemic, such as sex and age, should be kept confidential and the personal information should be destroyed when there is no more need for the information (Song, 2020). This legislative revision confirms Davis' (2009) argument that the extent of privacy protection depends on collective sensitivity and consensus with respect to privacy issue in a society.

3.2. Self-Quarantine Safety Protection App: Accountability for health conditions

Self-Quarantine Safety Protection App (hereafter, the App) was developed and used by the Ministry of Interior and Safety (MoIS). MoIS developed two versions of the App: one for those self-quarantining and the other for public monitoring (MoIS, 2020a). The App was launched on 7 March 2020 to automatically monitor self-quarantining people's locations and health conditions for 14 days (MoIS, 2020b). As the App was developed by MoIS[vii] concurrently with the System, we see a rhizomatic arrangement of the surveillant assemblage. How did this happen?

A user guide published in English by the Ministry of Foreign Affairs[viii] (MoFA, 2020a) illustrates how the App monitored those self-quarantining. While they were required to install the App on their smart phones, their locations must be made known, be available for calls from public servants assigned to them, and give consent to the collection and use of their personal information including their name, date of birth, sex, nationality, mobile phone number, and self-quarantine address. This information was then shared with other institutions composing the surveillant assemblage, such as local councils administering an area to which the quarantine address belonged. According to the MoHW's Covid-19 Response webpage, this information sharing aimed "to strengthen the monitoring system" (MoHW, 2020a).

To ensure that those self-quarantining always carry their phones, public servants in their local councils called them randomly once or twice a day, and when the phone stays put for a long

period of time (usually 3 hours during day time), an alert message was sent to the public servant while the phone beeping. If they left the selected quarantine place, both the phone users and the public servants would be notified of this movement so that the public servant would encourage the self-quarantine breaker to return to the self-quarantine place. Failing this, the Police would enforce the self-quarantine (MoIS, 2020a). So, the App also territorialised local councils and the Police and those self-quarantining were held accountable to the App for their locations to mitigate possible future risk of Covid-19 infection and transmission that their body might bear.

Hence, the App users must report at least twice a day (alarm went off twice a day for this purpose) regarding their Covid-19 symptoms such as body temperature (37.5° Celsius or higher), cough, sore throat, and respiratory difficulties or breathlessness. Consequently, those who closely contacted a Covid-19-confirmed body had to self-quarantine and report every day to KCDC via the App for 14 days about their location and health condition. In this way, the limit of accountability was being pushed: these individuals were now held accountable for possible future risk of Covid-19 transmission.

Moreover, this practice was extended to inbound travellers as special entry procedures comprising post-entry test, quarantine, and monitoring were implemented (MoHW, 2020c). Inbound travellers were Covid-19 tested upon arrival and, if the result was negative, they were required to self-quarantine for 14 days, and then their locations and health conditions were monitored via the App[ix]. Just like other App users, they must daily report their health conditions for 14 days from the arrival date (MoHW, 2020a). Prior to the arrival in Korea, the travellers were advised by KCDC (2020) of this requirement.

KCDC (2020) emphasised the possible consequences of non-compliance of the requirement: "[i]f you do not fully comply with those stated above, you will face up to 1 year [incarceration] or a 10-million won fine (approximately EUR 7,000) in accordance with the relevant laws." They were reminded of this by the *Travel Record Declaration Form* they had to fill in upon arrival. This form emphasised:

> If you leave your quarantine area without permission during your home quarantine period or otherwise fail to comply with quarantine guidelines [including daily reporting health status via the App], you will be required to wear a safety band on wrist. If you still refuse to comply, you will be ordered to quarantine at a facility (*You may be required to pay for the use of the facility) (MoFA, 2020b).

So, the inbound travellers' use of the App during the self-quarantine period was not merely a recommendation but legal enforcement. Cases of those fined for leaving the self-quarantine area often reported by the press (Jang, 2020). In this way, inbound travellers, regardless of their nationality, were held accountable to the surveillant assemblage for their body not because of their own current health conditions but due to the possible future risk of Covid-19 infection and transmission their body might bear. Hence this practice also pushed the limit of accountability.

4. Discussion and conclusion

We illustrated how BDA pushed the limit of accountability. We found that BDA enabled the surveillant assemblage comprising the System and the App to be constructed and operationalised rhizomatically. It rhizomatically territorialised several central government departments such as MoLIT, MoSI and MoIS, in addition to MoHW which KCDC belongs to, and 120 public and private agencies during the System development phase. During its operational phase, three telecommunications service providers and 22 debit/credit card companies, the Police, and local

councils were also territorialised in addition to public and private medical centres. Hence, this surveillant assemblage harnessed both public and private information to enforce accountability. Within the social and environmental accounting literature, despite its implicit assumption, no single set of information can produce corporate sustainability reports: rather they are produced from both private and public databases (Leong and Hazelton, 2019).

What we found was that the surveillant assemblage was constructed in a non-central rhizomatic manner. It was enabled by BDA forming the state-form. That said, while the System was being developed, the MoIS independently developed the App to monitor the location and health conditions of those self-quarantining – another key component of the surveillant assemblage. When personal data collected by the surveillant assemblage was disseminated, the assemblage territorialised groups of people independent of the government who further processed the data and made it more user-friendly in forms of webpages and mobile applications. And desires drove this territorialisation: the government desired to enhance its legitimacy and approval rate by controlling the pandemic while the citizens desired to maintain their health and safety. So, the technologies originally designed to discretely monitor only their own target objects were now encroaching an uncharted territory: the previously taken-for-granted value of privacy. Although this may provoke a moral question, it pushed the limit of accountability.

We contribute to debate on the limits of accountability (Messner, 2009). The surveillant assemblage held individuals accountable for their location and their biometric attributes such as body temperature due to possible future risks of Covid-19 infection and transmission their bodies might bear, due not to actual infection. It is the surveillant assemblage which can push the limit while the state-form reinforce the society of control, subjectivising individuals who understand that they are being monitored by that assemblage.

We also contribute to the newly emerged Deleuzo-Guattarian accounting studies which theorised controls in relation to overall functioning of societies of control (Carter and Whittle, 2018; Munro and Thanem, 2018). We argue that it is the BDA-enabled surveillant assemblage that facilitates a SF in societies of control. We hope that other researchers may explore how this would happen in different trajectories of SF.

There is a social implication as well. We found that individuals are held accountable to the surveillance assemblage for their locations and health conditions at the expense of their privacy. The mass may consider to what extent individuals' personal information should be protected and how to hold the governments accountable for the legitimate use of such information. (Davis, 2009; Fuch, 2009).

References

Alawattage, C., Graham, C. and Wickramasinghe, D. (2019), "Microaccountability and biopolitics: Microfinance in a Sri Lankan village", *Accounting, Organizations and Society*, Vol 72, pp. 38-60.

Andreassen, R. (2020), "Digital technology and changing roles: A management accountant's dream or nightmare?", *Journal of Management Control*, Vol. 31, pp. 209-238.

Arnaboldi, A., Busco, C. and Cuganesan, S. (2017), "Accounting, accountability, social media and big data: revolution or hype?", *Accounting, Auditing & Accountability Journal,* Vol. 30 No. 4, pp.762-776.

Carter, C. and Whittle, A. (2018), "Making strategy critical?", *Critical Perspectives on Accounting*. Vol. 53, pp. 1-15.

Chang, S., Pierson, E., Koh, P., Gerardin, J., Redbird, B., Grusky, D. and Leskovec, J. (2020), "Mobility network models of COVID-19 explain inequities and inform reopening" *Nature*, 1-26.

Davis, S. (2009), "Is there a right to privacy?", *Pacific Philosophical Quarterly,* Vol. 90 No. 4, pp. 450-475.

Deleuze, G. (1992), "Postscript on the societies of control", *October*, Vol. 59, pp. 3-7.

Deleuze, G. (1995). *Negotiations, 1972-1990*. Columbia University Press, New York.

Deleuze, G. and Guattari, F. (1987), *A Thousand Plateaus*, University of Minnesota Press, Minneapolis.

Deleuze, G. and Parnet, C. (2007), *Dialogues II,* Columbia University Press, New York.

Fuchs, C. (2011), "Towards an alternative concept of privacy", *Journal of Information, Communication and Ethics in Society*, Vol. 9 No. 4, pp. 220-237.

Haggerty, K. and Ericson, R. (2000), "The surveillant assemblage", *The British Journal of Sociology*, Vol. 51 No. 4, pp. 605-622.

Lee, D. and Lee, J. (2020), "Testing on the move: South Korea's rapid response to the COVID-19 pandemic", *Transportation Research Interdisciplinary Perspectives*, Vol. 5, 100111.

Leong, S. and Hazelton, J. (2019), "Under what conditions is mandatory disclosure most likely to cause organisational change?", *Accounting, Auditing & Accountability Journal*, Vol. 32 No. 3, pp. 811-835.

Mayer-Schonberger, V. and Cukier, K. (2013), *Big Data: A Revolution that will Transform How we Live Work and Think*, John Murray, London.

Messner, M. (2009), "The limits of accountability", *Accounting, Organizations and Society,* Vol. 34 No. 8, pp. 918-938.

Moffitt, K. and Vasarhelyi, K. (2013), "AIS in an Age of Big Data", *Journal of Information Systems*, Vol. 27, No. 2, pp. 1-19.

Moll, J. and Yigitbasioglu, O. (2019), "The role of internet-related technologies in shaping the work of accountants: New directions for accounting research", *The British Accounting Review*, Vol. 51 No. 6, 100833.

Munro, I. and Thanem, T. (2018), "Deleuze and the deterritorialization of strategy", *Critical Perspectives on Accounting*, Vol. 53, pp. 69-78.

O'Dwyer, B. and Unerman, J. (2007), "From functional to social accountability: Transforming the accountability relationship between funders and non-governmental development organisations" *Accounting, Auditing & Accountability Journal*, Vol. *20* No. 3, pp. 446-471.

Park, S., Choi, G. and Ko, H. (2020), "Information technology–based tracing strategy in response to COVID-19 in South Korea—privacy controversies". *JAMA,* Vol. 323 No 21, pp. 2129-2130.

Roberts, J. (2009), "No one is perfect: The limits of transparency and an ethic for 'intelligent' accountability", *Accounting, Organizations and Society,* Vol. 34 No. 8, pp. 957-970.

Roberts, J. and Scapens, R. (1985), "Accounting systems and systems of accountability: Understanding accounting practices in their organisational contexts", *Accounting, Organizations and Society*, Vol. 10 No. 4, pp. 443-456.

Vasarhelyi, M., Kogan, K. and Tuttle, B. (2015), "Big Data in accounting: An overview", *Accounting Horizons,* Vol. 29, No. 2, pp. 381-396.

Appendix 1: Data sources

Bicker, L. (2020), "Crushing the Curve", *BBC News* (10 May 2020) (available at https://www.bbc.co.uk/news/av/world-asia-52584494/coronavirus-how-south-korea-crushed-the-curve Accessed 17 July 2020).

Gallop Korea, (2019), *Survey Result of the Use Rate of Smart Phones, Brands, Smart Watches, and Wristwatches,* (available at https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1041 Accessed 1 July 2020)

Jang, A. (2020), "Self-quarantine breakers are published for going to work and beach", Yonhap News Agency (15 November 2020) (available at https://www.yna.co.kr/view/AKR20201114042500054?input=1195m Accessed 7 December 2020)

Kasulis, K. (2020), "S Korea's smartphone apps tracking coronavirus won't stop buzzing*", Al Jazeerah* (9 April 2020) (available at https://www.aljazeera.com/news/2020/04/09/s-koreas-smartphone-apps-tracking-coronavirus-wont-stop-buzzing/ Accessed 7 December 2020).

KCDC, (2020), *For Entrants to Korea: Instructions for Quarantine Subjects*, Korean Centre for Disease Control and Prevention (available at http://overseas.mofa.go.kr/gb-en/brd/m_8338/view.do?seq=761355&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1 Accessed 5 June 2020).

KHARN, (2020), "Covid-19 Smart Management System developed by KAIA", *Korean Heating, Airconditioning and Renewable Energy News* (29 March 2020) (available at http://www.kharn.kr/news/article.html?no=12345 Accessed 19 June 2020)

Kim, H. (2020), "Coronavirus privacy: Are South Korea's alerts too revealing?" *BBC News* (5 March 2020) (available at https://www.bbc.co.uk/news/world-asia-51733145 Accessed 8 July 2020)

MoFA, (2020a), *User Manual for Self-Quarantine Safety Protection App,* Ministry of Foreign Affairs (available at http://overseas.mofa.go.kr/us-houston-en/brd/m_5573/view.do?seq=759763 Accessed 5 June 2020).

MoFA (2020b), *Travel Record Declaration Form,* Ministry of Foreign Affairs (available at http://overseas.mofa.go.kr/gb-en/brd/m_8338/view.do?seq=761355&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1 Accessed 5 June 2020).

MoHW, (2020a), *Covid-19 Responses,* Ministry of Health and Welfare (available at http://ncov.mohw.go.kr/en/baroView.do?brdId=11&brdGubun=111&dataGubun=&ncvContSeq=&contSeq=&board_id=&gubun= Accessed 4 June 2020).

MoHW, (2020b), *Self-Diagnosis App. Manual for Instructors,* Ministry of Health and Welfare (available at http://ncov.mohw.go.kr/shBoardView.do?brdId=3&brdGubun=32&ncvContSeq=556 Accessed 1 July 2020)

MoHW, (2020c), *COVID-19 and Korea's Response,* Ministry of Health and Welfare (available at https://youtu.be/sFSr6tosDkE Accessed 3 December 2020)

MoIS, (2020a), "Q&A about Self-Quarantine Safety Protection App", *Press Release by the Ministry of Interior and Safety* (5 March 2020) (available at https://www.mois.go.kr/frt/bbs/type002/commonSelectBoardArticle.do;jsessionid=7bA+UtY0JOIXJytznXoyYNHR.node40?bbsId=BBSMSTR_000000000205&nttId=76155 Accessed 1 July 2020)

MoIS, (2020b), "Self-Quarantine Safety Protection App was found effective for self-quarantine", *Press Release by the Ministry of Interior and Safety* (21 March 2020) (available at https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=76366, Accessed 1 July 2020).

MoLIT, (2020a), "Developing Covid-19 Smart Management System", *Press Release by the Ministry of Land, Infrastructure, and Transportation* (10 March 2020) (available at https://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?lcmspage=1&id=95083656 Accessed 19 June 2020)

MoLIT, (2020b), "Press Conference on Covid-19 Smart Management System", *Press Release of the Ministry of Land, Infrastructure, and Transportation* (10 April 2020), (available at http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?lcmspage=6&id=95083773 Accessed 19 June 2020)

Policy Briefing (2020), "Press Conference on Covid-19 Smart Management System", *Republic of Korea Policy Briefing by the Ministry of Culture, Sports and Tourism* (available at http://www.korea.kr/news/pressReleaseView.do?newsId=156385019&call_from=seoul_paper Accessed 19 June 2020)

Song, J. (2020), "Coronavirus and personal data protection", Babytimes (1 December 2020) (available at http://www.babytimes.co.kr/news/articleView.html?idxno=41422 Accessed 7 December 2020)

Watson, I. and Jeong, S. (2020), "Coronavirus mobile apps are surging in popularity in South Korea", *CNN News* (28 February 2020) (Available at https://www.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html Accessed 24 June 2020).

[i] Korea had the second wave in August and was going through the third wave in November 2020. However, 29 February 2020 still shows the highest number of confirmed cases in one day. As of 1 December 2020, MoHW (http://ncov.mohw.go.kr/en) reported 34,652 cumulative confirmed cases, amongst whom 27,885 have been released from isolation, 6,241 are still being isolated, and 526 have deceased.

[ii] KCDC was renamed Korea Disease Control and Prevention Agency in September 2020.

[iii] The fact that this press conference was not held by The Central Disaster and Safety Countermeasure Headquarters, the official central control tower, nor by MoHW but by MoLIT suggests that the development and operation of the System was not centrally arranged but was rhizomatic.

[iv] Both the total population and the number of smart phones being used in Korea were around 51 million in 2019 (Gallop Korea, 2019).

[v] The pop-up notice window presents the names of individuals who contributed to the development and operation of the website.

[vi] The pop-up window indicates that Corona-live is not an official but privately-run website.

[vii] MoIS is equivalent to Ministry of Home Affairs of other countries, but "Safety" was added to its name because MoIS oversees firefighting and policing systems.

[viii] This indicates that MoFA was also rhizomatically connected to the surveillant assemblage.

[ix] A small number of travelers, in particular those on diplomatic visa, were exempted from the use of the App. Instead they were required to install another application called Self-Diagnosis App, which did not include the function of daily reporting of health condition for 14 days (MoHW, 2020b).