

COVID-19 and the decline of autonomy: contact tracing in the age of surveillance capitalism.

Stephanie Manne, MNNSTE011



A minor dissertation submitted in partial fulfilment of the requirements for the award of the degree of Master of Social Science in Politics

Supervised by Dr Gavaza Maluleke
Faculty of Humanities
University of Cape Town

Words: 25218

2022

DECLARATION:

1. I am presenting this dissertation in FULL fulfilment of the requirements for my degree.
2. I know the meaning of plagiarism and declare that all of the work in the dissertation, save for that which is properly acknowledged, is my own.

I hereby grant the University of Cape Town free licence to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever of the above dissertation.

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

Contents

Abstract.....	4
Chapter 1: Introduction.....	5
1.1. Background.....	5
1.2. Literature Review.....	7
1.3. Theoretical Framework.....	9
1.4. Research question.....	15
1.5. Methods.....	16
1.6. Limitations.....	17
Chapter 2: The dangers of evolving surveillance technologies.....	19
2.1. Defining surveillance.....	19
2.2. Human rights concerns of surveillance and health surveillance technologies.....	20
2.3. Surveillance abuse and the “function creep”.....	22
2.4. Surveillance maintains and strengthens the modern welfare state.....	26
2.5. The chilling effect: losing privacy and freedom to digital surveillance.....	29
2.6. Technological developments behind surveillance today.....	31
2.7. A new world order under surveillance capitalism.....	34
Chapter 3: New forms of digital health surveillance during COVID-19.....	43
3.1. Introducing contact tracing applications.....	43
3.2. How contact tracing applications work.....	45
3.3. Distinguishing safe and unsafe bodies through contact tracing technologies.....	46
3.4. Regulatory gaps in contact tracing technologies.....	48
3.5. Contact tracing applications in practice: the case of Asia.....	51
3.6. Approaching data privacy.....	53
3.7. How Taiwan and South Korea developed successful pandemic responses.....	55
3.8. Why preserve democracy?	59
3.9. Making sense of the fears behind contact tracing applications.....	62

3.10. Contact tracing as technological solutionism: the system of surveillance capitalism.....	65
3.11. The consensus on contact tracing applications in the COVID-19 pandemic.....	68
Chapter 4: Conclusion.....	71
4.1. Why contact tracing applications fail.....	71
4.2. Why democracy and human rights fail.....	73
References.....	77

Abstract

To develop successful COVID-19 pandemic response models, governments and policy makers are expanding on the known means of public health surveillance by collaborating with privately owned corporates and implementing new forms of surveillance technology, namely, contact tracing applications. This study examines the long-standing history of surveillance as well as the shifts in public health surveillance with the rise in technologically mediated solutions. In both research and public discourse, the overriding conversation is around the preservation of democracy and human rights and fearing the loss of “freedom” to the adoption of COVID-19 surveillance technologies. After analysing a series of academic journals and news articles that have been published since the beginning of the pandemic, this study highlights how a widespread use of such technologies has been encouraged in the name public health and safety, despite existing evidence of the shortfalls of contact tracing applications. By understanding the fundamental failures of democracy and the inequality that it perpetuates, this study argues that in the same way that the COVID-19 pandemic requires the creation of safe and unsafe bodies, so too does the system of democracy which depends upon creating fear and insecurity so that a reliance on the state is strengthened. As a result, the COVID-19 pandemic is accelerating a world of technological solutionism and surveillance that yields very unequal social, political and economic power dynamics wherein biology and personal data are exploited and commodified. This study employs of the theoretical frameworks of Foucault in making sense of the politics behind pandemic response models and the guiding roles of power, governmentality and biopower. While outlining the dangers of surveillance capitalism, this study makes sense of the push to rely on and preserve the system of global capitalist democracy.

1. Introduction

1.1. Background

On March 11, 2020, the World Health Organization officially declared the novel coronavirus a pandemic. Since then, countries have been scrambling to develop a successful pandemic response model, including the development of an effective vaccine. Different government monitoring tools have been implemented in attempt to safeguard public health which ultimately determines social stability and the preservation of the national economy. These emergency tools each have an element of threat to one's freedom, right to privacy and role of political participation (Greitens, 2020: 170). Combined with a very limited understanding of and experience with COVID-19, there is a great sense of resistance and fear surrounding the loss of freedom and human rights within democracies worldwide.

Governments have displayed different levels of preparedness, introducing varied measures of social distancing to limit the spread of virus infection. Behavioural responses to limit the spread of the infection are ultimately judged by the economic costs attached to them (Osman et al., 2020: 55). Government responses to contain the spread of this highly communicable disease have, in some instances, been strict and closely monitored through lockdowns, where citizens are strictly confined to their homes and only essential grocery shopping. Lockdowns therefore disallow the freedom of assembly and one's freedom of movement by restricting national and international travel. Other less strict and daily measures to limit the spread of the virus have included mandatory sanitizing when entering public spaces and the government encouragement to improve personal hygiene. Mask wearing, protective clothing, social distancing, self-isolation, quarantines, and testing have all been enforced as COVID-19 protocol.

During this time digital technologies have gained momentum as supplementary tools to the more traditional containment efforts. Contact tracing applications are a surveillance and containment effort to limit the spread of the virus which work to identify where the infection originated and the path that it takes in terms of community infection (Osman et

al., 2020: 56). Contact tracing is punted for its ability to monitor the spread of the virus in real time. International corporations have desperately pursued different efforts alongside national governments to develop an effective digital contact tracing model. However, real-time mass monitoring is also synonymous with population control (Kitchin, 2020: 362). Within less than a year, governments have had to re-evaluate and implement emergency public health policies and health surveillance measures that pertain to health data sensitivity, privacy, and protection (Greitens, 2020: 169). Therefore, emergency pandemic responses have had varying impacts on national approaches to surveillance, democratic principles, and individual freedoms. The emergency government responses to the COVID-19 pandemic have sparked academic debate surrounding concerns for the abuse of surveillance technologies in the future. More so, how these measures that are emerging out of the pandemic may change the patterns of democratic leadership.

Having originated in China, Asia as a continent has been a step ahead of the world in developing some of the first COVID-19 response models (Greitens, 2020: 170). China has also displayed how pre-existing authoritarian leaderships are being strengthened through the COVID-19 pandemic and the mandating of intelligent surveillance technologies, legitimising the worldwide concern for the spread of illiberal leadership. However, Asia's advantage in pandemic response has also been a result of working on its pandemic response models since the devastation many of its countries faced from the outbreaks of SARS in 2003 and then the Middle East Respiratory Syndrome (MERS) in 2012 (Fahey and Hino, 2020: 3).

As a result, South Korea, Taiwan, China, Hong Kong and Singapore were some of the quickest moving countries to implement contact tracing strategies due to experience of needing to track and trace the virus in its early stages. Interestingly, the Asian continent has produced some of the most divergent pandemic responses. Therefore, it has been a useful space of study in demonstrating how pandemic response models have the potential to shape the future of the political system. A common assumption would be that the pandemic response will likely reflect or strengthen the existing political regime. Debate on how the pandemic may shift the existing patterns and understandings of democracy

has been rife. Where democratic standards have been violated, there has been a widespread concern for the spread of illiberal leadership and surveillance potentialities in life beyond the pandemic.

1.2. Literature Review

As it stands, the available literature on contact tracing efforts in the time of COVID-19 have celebrated the efforts of the Asian Tigers. There is a large body of work that frames the digital contact tracing responses of these countries as models off which the rest of the world should base its public health responses. Taiwan's pandemic response has been widely praised in political debates and across media platforms worldwide for developing a successful pandemic response model. Reports on its collaborative governance and digital democracy share how Taiwan could be used as a pandemic response model for democracy in the rest of the world. In the same breath, there is a significant volume of academic literature on state surveillance and its ability to control communications and censor important information, particularly in times of crisis.

While surveillance is an age-old tactic used by states to monitor its populace, surveillance today has reached new heights. In recent history, rapid developments in daily technologies have led to many unexpected advances in surveillance potentialities. As technologies are constantly being developed, people are becoming more aware of how digital surveillance is changing the shape of the world. One of the first big public scandals that brought the issue of surveillance in the 21st century to light was in 2013, when Edward Snowden, an employee of the United States National Security Agency exposed how the state had been wrongly capitalising on the surveillance of its people by monitoring daily digital communications and blatantly infringing on one's right to privacy. Consequently, Snowden highlighted how the world fell victim to the function creep of surveillance. A significant amount of research and debate has therefore gone into the issue of state surveillance and the human rights implications, particularly on privacy. The Snowden revelations have initiated a large body of research on the contemporary conundrums of big data practices and the strengthening of surveillance. Central to a lot of the research

that has been done is the argument or belief that a human rights framework is necessary to protect the public from regulatory overreach of surveillance technologies (Sekalala, Dagon, Forman and Meier, 2020: 7).

Nevertheless, the world was caught off guard again in 2018, when it was uncovered that Cambridge Analytica and Facebook were abusing personal data from a social networking site to influence marketing schemes and manipulate the results of national presidential elections. Personal data was therefore improperly obtained from a third-party application to provide analytical assistance to presidential campaigns in the United States. As a form of digital surveillance, such incidences have confirmed the forms of psychological targeting and democratic erosion that scholars have been warning against for years. This scandal saw a shift in the literature which began to focus on the role of personal data as a raw material and a commodifiable entity, focusing on the important role of surveillance in the contemporary strain of capitalism (Fahey and Hino, 2020).

Naturally, digital contact tracing in the time of COVID-19 has also sparked concern for the likelihood of surveillance creep and the consequences it may give way to. Contact tracing applications are being rushed into existence with a lack of widescale implementation, testing and policy. In many instances, contact tracing apps are significantly threatening democratic principles and basic human rights. As a result, scholarly debate on the illiberal potentials of COVID-19 response measures like national lockdowns and other emergency laws that may threaten bodily autonomy are rife in the literature.

Numerous studies have also conducted research on the issue of privacy in the post-pandemic world. These studies focus on the irreversible damage that the adoption of contact tracing measures may cause for the future of one's privacy, and are therefore focused on issues of privacy and data protection (Fahey and Hino, 2020). The available literature that addresses issues of privacy and the advancement of surveillance do so from the perspective of a dominant mainstream academic understanding of democracy. Therefore, this study will employ a different theoretical framework that aims to understand the creation of a system that has enabled such politics of exclusion. This study will

demonstrate how liberal capitalist democracy is a space of regulation and mediation of societal relations, within which its citizens are restricted to “narrow confines of behaviour and subjectivity” (Agathangelou, 2008: 131).

While there is research that addresses the issue of surveillance in context of the COVID-19 pandemic and the introduction of contact tracing applications, there is a gap in the literature that fails to address the marriage of surveillance capitalism and technological solutionism with contact tracing technologies in the face of the COVID-19 pandemic. More specifically, the available literature on Asia tends to celebrate its successes in forging ahead with contact tracing applications. This study aims to fill a gap in the existing body literature by paying attention to how, in this context, the world is being divided by “safe” and “unsafe” bodies, which is therefore contributing to an intensification of social and economic disparities. What is more, the available literature that looks at the issues surveillance and contact tracing together has failed to look at the questions of why and how this has been made possible. This study will address such questions using the Foucauldian perspectives of biopower and governmentality and Agathangelou’s (2008) understanding of citizenship and belonging within a democracy.

1.3. Theoretical framework

This study is particularly focused on the relevance of Foucault’s conceptions of power, discipline and surveillance and their significance in understanding the behaviour of states as well as the social responses to them. Closely connected to the dynamics of biopower, Foucault’s notion of governmentality is employed in this study’s analysis of the surveillance state and the savings technologies that have been adopted to curb the spread of the COVID-19 pandemic. It looks at how the state governs and how the people more strictly police one another and themselves (Muller, B. J., 2011: 4).

Central to this understanding is the functioning of liberal democracy, which will be employed using Foucault's understanding of democracy as a set of historically contingent practices that goes beyond a normative approach to the concept (Olssen, 2007: 205).

This study uses his work to understand the significance of relational power dynamics of liberal democracy and the critical role of agency, liberty, autonomy, and interdependence between individuals and the state (Olssen, 2007: 205).

It is also essential that one acknowledges the role of liberalism in Foucault's analysis of the "conduct of conduct", otherwise known as the politics between governing the self, the population, and the state (Muller, B. J., 2011: 8). Liberalism, closely tied to democracy, is focused on the welfare of a population and the governing over life. Thus, the values of wealth, longevity and the association of good healthcare are all supported by liberalism through freedom (Muller, B. J., 2011: 8). Similarly, the notion of free choice is regarded as an essential regulatory and disciplinary strategy, falling under the broader umbrella of governmentality. With this understanding in mind, if one fears to engage in the freedom of expression, one is inhibited from expressing their individualism and, in turn, developing as autonomous individuals who are key players in a democratic system and its processes (Murray and Fussey, 2019: 51).

This study will address these fears from a human rights perspective, using the framework of the European Convention of Human Rights (ECHR) as one of the most widely respected human rights bodies in the world (Bernal, 2016: 244). While the human right to privacy is often and quite obviously infringed upon, this study will look at which other human rights are perhaps more covertly intruded on. Human rights were developed to protect citizens from state interference to individual freedoms (Kosta, 2020: 2). They cover a broad spectrum of rights that are acknowledged through international treaties and organizations, particularly democracies worldwide (Kosta, 2020: 2). Rights-based concerns have naturally evolved out of the growth of surveillance technologies, with contact tracing applications posing significant threats to the protection of human rights at large.

Foucault (1978) argues that the concern surrounding power over the significance of one's life for the sake of population management is what one may refer to as biopower. Foucault's understanding of biopower as the power over life makes reference to the

constitution of and the control over the population that is comprised of individual bodies. These bodies are, in turn, capable of being put to work but also made to remain docile. This also applies to the aspect of biopower that concerns itself with physiological health and well-being, otherwise referred to as the governance of the self (Muller, B. J., 2011: 7). When implemented, biopower becomes biopolitics, which is materialised through the ways in which the state maintains control over human life through different measures like mandatory health check-ups (Kalpokas, 2020).

This study will analyse the developments in biopower as a strategy used to govern life. It will look at the power the state holds over individual and collective life, and the dangers of its proliferation in a world that is furiously scrambling to find solutions, at whatever cost, to preserve the national and international economies. This study will then look at the system of surveillance capitalism and the role of biopower in a COVID-19 world, looking at the power dynamics of the intersections between biology and politics, where social and political power are considered to be more important than individual life (Muller, B.J., 2011: 1).

According to Foucault (1978: 137), this has always been a privilege of sovereign power; to have the right to make choices about life and death. Biopower is a politics that depends upon the control, domination, and exploitation of the subjects over whom power is exercised, namely, the populace (Rabinow and Rose, 2006: 198). People also expect and trust that the state will work to save them, feeding the power that the state has over its people. At the same time, the state relies on its populace, wanting it to implement measures to look after them. This is fundamental to the narrative of saving.

The narrative of saving is used to confirm existing power dynamics between the populace and the state, ensuring trust and confidence in the belief that the state has the welfare of the people at heart. Thus, the narrative of saving essentially creates a blind following or support through which decisions by the state are left unchallenged. Meanwhile, the state is dependent upon the population to exert its control. This power dynamic underpins the functioning of democracy today and has led to mounting chaos in the global capitalist

system with a growing insurgency from below. Political protesting by minority groups who fear even worse oppression are contributing to the destabilisation of the world capitalist order, pushing the world to question and reimagine the current system. Consequently, there is an increasing sense that democracy can no longer be relied on to deliver its core promises nor uphold fundamental human rights.

The power dynamics of these relations can be made sense of through the elusive nature of power in politics as captured in Foucault's (1991: 194) perception of it. Power is a force in circulation and in relational terms (Foucault, 1991: 194). Without any specific agency or structure, power is a social and a political phenomenon that is present in every moment or interaction. This very reality has naturalised what one understands to be a power dynamic as well as the extent that humans discipline themselves and one another without the need for coercion by the state (Foucault, 1991: 196). In fact, Foucault (1991: 196) has highlighted how such power dynamics and notions of self and social discipline emerged out of 18th century Europe and its institutions. This study pays close attention to this naturalized dynamic within democracies and how the COVID-19 pandemic has exposed this docile and disciplined behaviour of populations at large.

Through a rigorous analysis of the modern bureaucratic state and its various institutions, Foucault saw the population as a collectively docile group of individuals who are together disciplined through the very existence of the above-mentioned institutions. Within these institutions, norms and values exist, which have created boundaries for what is considered to be delinquent or abnormal relative to what is accepted as the norm (Muller, B. J., 2011: 3). Through this process, one self-disciplines without being coerced to do so. Governmentality is closely linked to the above-mentioned reference to power and the ways in which governing is integral to the production of knowledge and ultimately, the establishing of "regimes of truth" (Muller, B. J., 2011: 5). This research is also interested in the correlation between the subject of governmentality and that of liberalism. Governmentality looks at the dynamics through which government directs behaviour, resulting in certain conduct or acts by the subjects of government (Muller, B. J., 2011: 4).

Commenting on the way that the power of the gaze forces individuals to conform to societal norms without need for coercion but rather through self-discipline that it encourages, Foucault (1979) lamented that:

“it is not necessary to use force to constrain the convict to good behaviour, the madman to calm, the worker to work, the schoolboy to application, the patient to the observation of the regulations ... He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection.”

This essentially refers to the fact that the existence of surveillance itself is secondary to its potential disciplinary effects (Muller, B. J., 2011: 3). Similarly, this study points out that in the context of COVID-19, citizen behaviour is dominated by a governmentality that accepts emergency health responses despite the potential limiting of human freedoms. Without the need for constant coercion, there is an unspoken agreement amongst a vast majority of world citizens that COVID-19 protocol will be followed. People stay home, wear masks, socially distance, and download the contact tracing applications, engaging in the process of self-discipline without necessarily being coerced into doing so. This very framework is employed to theorise the ways in which growing surveillance technologies are enforcing self-restraint that is ultimately threatening the fundamental values of a free democracy.

Foucault's insight into the emerging power dynamics at play that are produced by modern surveillance technologies as well as his use of Bentham's notion of the panopticon are perhaps more relevant today than ever before. Since the publication of *Surveiller et Punir* in 1975, Foucault has been a primary foundational thinker on the subject of surveillance (Manokha, 2018: 219). Foucault's conception of the power of the gaze can be used to describe both the repressive nature of an authority but also the dimension of self-discipline and self-restraint that it creates (Manokha, 2018: 221). The awareness that

there is a possibility one is being watched or monitored creates a process of self-restriction whereby one fears to express difference of opinion or individuality, enforcing self-discipline (Muller, B. J., 2011: 3).

Foucault (1981) acknowledged the repressive nature of Panoptic dispositifs which he later referred to as the technologies of the self. He analysed the ways in which panoptic settings result in people acting on and disciplining themselves, resulting in self-restraint (Manokha, 2018: 220). Foucault's work preceded the literature that labelled the "panopticon" as such. However, he had been studying and writing on the phenomena of these panoptic settings for many years where he emphasised the role of power in "the power of the gaze" within medical asylums or institutions and the power dynamics that emerged within these spaces (Manokha, 2018: 225).

Such institutionalised ways of being provide a very useful framework for making sense of different responses to the COVID-19 pandemic. In fact, Agathangelou (2008) is used to strengthen this analysis, providing a very rich literature off which this study bases its understanding of how the COVID-19 pandemic has exposed some very harsh realities of the world system. Agathangelou (2008: 120) complicates the common understanding of democracy to make sense of how, even under a supposedly free system, life is not at all free. However, citizens are willing to partake in the system in a hopeful exchange for a negotiated sense of belonging. This sense of belonging, safety and protection is dependent upon an imagined and created enemy (Agathangelou, 2008: 120).

Furthermore, Agathangelou (2008: 120) makes the argument that in order for people to believe that they are being saved requires the creation of an unsafe world. As a result, notions of governmentality are justified and strengthened. The state promises to honour its commitment to democracy and human rights based on the idea that it is protecting its citizens from the spread of illiberal tendencies or dangerous people. By and large, these democracies serve as part of the fundamentally unequal global capitalist system. By offering a different lens through which democracy may be understood, Agathangelou (2008) posits that; as an extension of the imperial project, democracy requires the

creation of an “other” (Agathangelou, 2008: 120). The other is necessary to confirm the belief that the democratic system is ensuring notions of safety, equality and freedom.

Consequently, in the time of COVID-19, emergency laws surrounding freedom of movement and the use of contact tracing applications are widely accepted despite their many downfalls. As a result, the pandemic has exposed and entrenched the harsh realities of the world system. Democracy, in particular, requires the negotiation of belonging within the global capitalist system. Thus, those who do not belong, or choose not to serve the interests of the state, are not protected by the state. On the contrary, they are further excluded and alienated from society. As states collaborate with private industry and commodify personal health data, an already unequal world system is exacerbated by oppressive and controlling new forms of technological solutionism. Which brings one to question what life ahead of the pandemic may look like in terms of bodily autonomy and the efficacy of contact tracing as a technological solution to the pandemic.

1.4. Research question

Contact tracing applications as an extension of government pandemic response plans have been rushed into existence despite their many flaws. Nevertheless, docile populations either cooperate and buy into the surveillance technologies, or are policed by other citizens to do so. The COVID-19 pandemic has exposed the stark inequities of the world while threatening the exacerbation of such realities. This study will address the disregard for human rights through national emergency laws as well as the prioritising of saving certain bodies over others. Contact tracing technologies are enabling exclusivity and surveillance as a measure to monitor and control populations. This study therefore aims to highlight and question the dangers of technological solutionism, but also the very system that enables such politics to occur. It does so by asking the question: What are the implications of introducing contact tracing applications on our understanding of democratic freedoms?

1.5. Methods

This study employed the method of secondary research in the form of academic articles as a primary source of data. The search strategy used neutral search terms including “digital” and “democracy”, “pandemic”, “contact tracing”, “surveillance” and “Asia” to identify academic articles on the related topic. The search criteria contained any of the above terms as well as the term “pandemic response” somewhere within the search titles. This search was limited to texts in English.

The parameters that have been set for this research project focus on national government’s responses to the pandemic and the use of digital technologies in their responses. With the given background, this study looked at different news reports, academic articles, journals, and reports by organisations among the likes of the World Health Organization. The data used for this research focuses on reports released within the first year and a half following the official first COVID-19 case. The time frame begins on 31st December 2019 when, according to the World Health Organization (2020), the Wuhan Municipal Health Commission first reported a cluster of similar cases of pneumonia in the Hubei Province (World Health Organization, 2020).

This research project has, however, used and analysed the continually updating world of news and academia that has been found to be of value in understanding and bettering the evidence for research. This is due to the unknown and constantly evolving nature of the research topic as well as the constant changes in the pandemic. The data collected thus far has come from a selection of news reports and opinion pieces on the Taiwanese, South Korean, Chinese, and Singaporean handling of the pandemic. The available information is thus relatively new, having been published in 2020 and 2021. The open-ended nature of this qualitative research study leaves room for new and unanticipated answers (Mohajan, 2018: 18).

In fact, the flexibility of this nature of research made it possible to follow and keep up to date with new, emerging and often unanticipated events and ideas throughout the

research process (Mohajan, 2018: 20). During the early stages of the research process, this therefore allowed for the direction as well as the framework of the research to be re-evaluated when new information and findings became available (Mohajan, 2018: 21). With a topic so new and under researched, this methodology was carefully selected to suit this research project. The chosen method holds a lot of value in leading to a deep analysis which leads to important insights on the topic, which have often come from probing at values, beliefs and assumptions around culture and society (Mohajan, 2018: 18).

Taiwan's digital democracy was found to be highly publicised and celebrated for its success in preventing the most collateral damage done to its people and system. The available research and media reporting on Taiwan is overwhelming supportive of the use of digitised contact tracing and pandemic response measures. This may have something to do with its status as one of the trailblazing "Asian Tigers" which alone is very stigmatised for its role as a pioneering nation.

1.6. Limitations

Due to the fact that the issue at hand is very recent, there is a lot of information and understanding that still needs to be reached as the volume of data available made it challenging to conduct an in depth as well as a well-rounded analysis (Mojahan, 2018: 16). The body of literature that addresses surveillance in the time of COVID-19 is limited, which interestingly may have a correlation with the social shaming that comes with opposing mainstream public health approaches. The infancy of the coronavirus also limits the data collection time frame to just over one year's worth of material. Ideally, a research project of this nature would have benefited from a few years of retrospection.

As it stands, there are limited academic research studies that have been done on the issue, nor has there been enough time to see the real ramifications happening on the ground. Nevertheless, because of the global sense of urgency to contain the coronavirus, there is a large volume of news and academic reports on the matter. In addition, there is

a significant body of literature on the public health interventions of previous SARS and MERS pandemics. Another limitation of discourse analysis in qualitative research is the constant need to evaluate the intentions and viewpoints of the news articles and academic journals studied, as well as those of the researcher responsible for conducting the project.

2. The dangers of evolving surveillance technologies

2.1. Defining surveillance

Since the beginning of the COVID-19 pandemic, there has been a global increase in the surveillance of populations to mitigate the spread of the virus. Being the first major global health pandemic in the information age, the COVID-19 coronavirus pandemic has become a testing ground for policy responses and savings measures using information and communications technologies (ICTS) (Fahey and Hino, 2020: 1). In this context, the role of private information and data becomes more valuable than ever as the world races to find the best possible solutions to contact tracing and vaccine passport technologies. At the end of the day, great economic reward and political power will be rewarded to whoever discovers or creates the best possible solution to mitigating the virus.

By definition, surveillance both forms part of and is a result of the processes of modernity (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 1). According to Lyon (2001), who has been central to the academic study of and conceptualisation of surveillance, the definition of surveillance ought to reflect the role of rational modernity behind it. He has thus referred to surveillance as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 2). Therefore, it is crucial that one understands the aspects of surveillance that are about monitoring, controlling and intervening in population behaviour. Systems of surveillance have historically been bolstered by technology, creating the potential for significantly greater and more detailed surveillance techniques (Lyon, 2007: 40). Surveillance measures are notorious for their ever-growing nature. A common surveillance mechanism is the "function creep", which refers to how techniques have historically been overused, drawn-out and twisted from their origin (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 2).

2.2. Human rights concerns of surveillance and health surveillance technologies

Dating back to the Industrial Revolution, nationalist governments used public health surveillance to legitimise discriminatory public health policy against migrant peoples. Like the COVID-19 pandemic, the quick transmission of disease in city centres and urban areas often blamed racial minorities. An example is how the spread of smallpox in San Francisco in 1876 was blamed on the Chinese Americans based in the city (Sekalala, Dagon, Forman and Meier, 2020: 10). Surveillance and policing thus targeted the Chinese population more generally, enforcing quarantines based on race. Furthermore, public health reports were published that blamed the outbreak of smallpox on the Chinese population for not assimilating themselves with Western society well enough. The spread of the disease was thus used to highlight and blame Chinese people living in America at the time, allowing and leading to further discrimination and stigmatisation of the population (Sekalala, Dagon, Forman and Meier, 2020: 10).

Similarly, the Holocaust genocide is known to have used surveillance tactics to pursue its agenda of deciding who has the right to survive and by justifying the killing of millions of people in the name of a national health emergency. The Holocaust agenda was executed using IBM Identification technologies to monitor and track down the populations it was after, mostly Jews, blacks and homosexuals (Lyon, 2007: 35). Ultimately, identification systems, otherwise referred to as surveillance systems, were used to decide who had the right to life, the essence of biopower.

When the Holocaust genocide was justified by a health concern on behalf of the German state that violated the rights of many minority populations, there was cause for an international consideration of the protection of people's rights. This was fostered through the United Nations organisation, which was focused on the importance of non-discrimination and equality as central aspects of international human rights law (Sekalala, Dagon, Forman and Meier, 2020: 10). The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights as well as the International Covenant on Economic, Social and Cultural Rights all work as bodies to ensure and protect human

rights and that state bodies do so without the interference of any kind of discrimination (Sekalala, Dagron, Forman and Meier, 2020: 10). Without becoming distracted from the main discussion here, the theoretical distinction of international should be made. This research study understands the international to incorporate the worldwide system of nation-states that conciliates the relations between classes (Robinson and Harris, 2000: 16). This includes the relations and flows of national capitals, particularly those of the bourgeoisie (Robinson and Harris, 2000: 16).

While the above-mentioned international organisations focus on the protection of privacy as a fundamental human right, the member states have discussed the necessary conditions that ought to reconsider the limiting or suspension of certain rights- like the right to privacy (Sekalala, Dagron, Forman and Meier, 2020: 10). Since then, public health crises or national emergencies have been considered grounds for certain rights to be limited. An issue materialised into the Siracusa Principles document, positing the specific conditions that may lead to the potential imposition of one's human rights (Sekalala, Dagron, Forman and Meier, 2020: 10). This would occur in very specific and very limited circumstances, with an issue of public health being one of them. The Siracusa Principles document is a nonbinding document developed by non-governmental organisations and adopted by the United Nations Economic and Social Council in 1984 (Sekalala, Dagron, Forman and Meier, 2020: 10).

The Siracusa Principles have been of great significance to understanding and respecting the critical link between the sphere of public health and that of human rights. Ultimately this speaks to the importance of aligning global health governance with human rights law, which is also highlighted in the International Health Regulations, a legal framework developed by state bodies throughout the world that is used to address public health emergencies (Sekalala, Dagron, Forman and Meier, 2020: 11). Despite the presence of such frameworks and the international concern for the marriage of human rights with global health governance, the development of digital surveillance technologies today continue to infringe on a host of human rights.

Of particular concern is the right to privacy, as well as the outlawing of discrimination of any kind. These concerns closely relate to the fact that surveillance technologies erode public trust as personal data is commodified and may be used for reasons beyond the public health emergency. Scholars have been questioning surveillance and its existence in society for as long as it has been visible and has been known to serve the interests of decision-makers within the state and the bureaucracy (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 2).

The discussion mentioned above has highlighted the historical abuse of public health surveillance by states to justify discrimination of minority populations. The commodification of data in the 21st century has also strengthened the surveillance potentialities of states, and vice versa. Consequently, states together with big tech are notorious for capitalising on and often abusing private data.

2.3. Surveillance abuse and the “function creep”

Public distrust and scepticism are genuine concerns surrounding the emergency savings measures used in the context of the novel COVID-19 coronavirus pandemic. There has still not been enough effort in the policy space to address the issue of surveillance in such circumstances of national health emergencies, raising the question of whether savings technologies are doing more harm than good. For many years now, there has been a growing divide between far-right and far-left political spheres (Robinson, 2020: 11). While the far-right groups have grown significantly in popularity, there is a reason for raising concern for the types of regimes that will attempt to capitalise on the COVID-19 health pandemic, which has sparked a wave of political activism and protest throughout the world.

The COVID-19 pandemic has highlighted the important and quickly growing surveillance tactics through the use of contact tracing measures in a world that is already threatened by the role of the "function creep" today. It has now been demonstrated that the issue of surveillance is not new. In fact, contact tracing technologies are not new either. Electronic

data systems effectively identified infection clusters in an emergency public health response to the Middle East Respiratory Syndrome (MERS) outbreak in Hong Kong in 2003 (Sekalala, Dagon, Forman and Meier, 2020: 9). Similarly, mobile phone data were used to identify travel patterns during the Ebola outbreak in West Africa from 2014 to 2016 (Sekalala, Dagon, Forman and Meier, 2020: 9).

Surveillance has been used to control and monitor populations for centuries (Lyon 2019: 69). Surveillance technologies that have been developing over these years are essentially born out of one another. Lyon (2007) has made the critical distinction in this work that surveillance is often mistaken as something new. He further highlights how problematic the obsession with the present is- a symptom of a culture of immediacy, causing a loss of cultural memory should one fail to look at the longstanding history of surveillance (Lyon, 2007: 33). Lyon (2007: 33) argues against the widespread assumption that technology has been the greatest driver of surveillance, but rather that it is simply one of the many instruments used to advance an already existing system of surveillance culture.

The pervasiveness of surveillance and the development of smart technology is arguably what has changed. Since the worldwide increase in security following the 9/11 attacks and the proliferation of social media, a new surveillance culture emerged (Lyon, 2019: 69). Since then, surveillance in the form of constant monitoring through the likes of video cameras in public spaces became naturalised as a part of everyday life. One may be watched and monitored in both public and private spaces, through security cameras in buildings and airports, in vehicles, through devices, all of which may collect, store, analyse and act upon the data collected (Lyon, 2019: 69).

What is spoken of here is a surveillance culture that has been a significant part of the facilitation and normalisation of evolving surveillance technologies. The normalisation of surveillance has been a process through which states and government authorities have introduced and tested a plethora of different surveillance measures under the justification that these have been either health savings or security savings measures. Thus, the

COVID-19 pandemic has vastly proliferated and normalised contact tracing measures and protocols that are widely accepted under the label of savings measures.

Before continuing with this discussion, one must identify the state in this context. This study uses a Foucauldian lens which sees the state as an assemblage of power relations at every level within the body of society. The state is a "scheme of intelligibility for a whole group of already established institutions and realities" (Foucault, 2006: 294). While Foucault has faced criticism for lacking an exact conception of the state, one must understand the very logic behind this, highlighting something else fundamental. That is, the state is a much bigger collection of power relations across all social groupings and extends way beyond the confines of the state.

The state cannot be characterised with a one-dimensional definition but should encompass the many levels and relational dynamics that create this entity. The state comprises a collective that has unanimously decided to follow society's rules and unspoken rules together. As a result, Foucault has paid particular attention to the role of governmentality, using the term to describe a way of being in control of populations in modern European history with the rise of the state (Sawyer, 2015: 138). Governmentality includes the techniques and means created to govern the behaviour of the individual and society at every level, the entirety of the state.

State surveillance measures and technologies have become so ubiquitous and normalised, leaving them often unchallenged. Wearable technologies and surveillance measures have seamlessly crept into life without mass awareness of their capabilities. Surveillance today looks very different to the more tangible surveillance tactics that have historically existed. Through these technologies mentioned above and the very ubiquity of surveillance, the measures used in daily life are creeping closer to becoming blatant threats to human rights like the right to privacy. Privacy infringement was indeed exposed through the events of the Snowden Leaks and, shortly after, the Facebook and Cambridge Analytica scandal, where personal data has been used to influence marketing schemes and election campaigns (Fahey and Hino, 2020: 3). These events have

demonstrated how surveillance potentialities today have entered new, unimagined horizons (Herrera, 2015: 354). Massive scandals surrounding the use of personal citizen data for illegal uses have given rise to growing concern and fear of digital surveillance. Not only does this threaten the idea of a free life under a liberal democracy, but it raises a question mark for the future living under an already authoritarian regime. Thus, the rapid advancements in surveillance measures under the guise of political savings ought to be thoroughly debated and questioned.

The issue with leaving these measures unchallenged is that it channels citizen trust toward the government rather than amongst one another. Ultimately, technology imagines a new type of community. In this community, the people trust the state, and the need for social trust has been obviated by the new technologically mediated form of social cohesion (Stevens and Haines, 2020: 530). As citizens happily opt for such forms of citizen science, there is less room for citizens to monitor and call for checks and balances within the government. There is thus concern around the future as social fragmentation will increase along with community distrust as citizens trust the government and not one another (Stevens and Haines, 2020: 530). This context of social fragmentation and government confidence creates the potential for surveillance measures to develop even further.

On the other hand, leaving such matters unchecked and enabling the development of surveillance tactics has created a world of fear and distrust. Individuals refrain from conducting particular online searches or from expressing their political opinion. This environment has been born out of the reality that governments and institutions monitor and troll specific individuals who may face potential consequences. This discussion bears particular relevance to the context of COVID-19 today and the introduction of emergency contact tracing measures in an attempt to contain the spread of the virus.

The normalisation of a culture of surveillance enables the very measures themselves to grow and develop. Surveillance has been a part of life for centuries, and this study has proven it to rear an ugly head, dating as far back as the Industrial Revolution and as

recently as the past five years. Surveillance today is more pervasive than ever, as wearable technologies constantly monitor and capture personal data relating to movements, voice recognition, facial recognition, and general behaviour. The capabilities of such measures raise a host of concerns, firstly, surrounding the preservation of privacy and individual autonomy over decision making. The adoption of invasive surveillance measures like contact tracing technologies threaten freedom of choice and bodily autonomy as citizens are tightly monitored and controlled by the state. To add to the greater tragedy, there is already an existing state of anxiety between citizens who fear the unknown of the global health pandemic and one's future.

2.4. Surveillance maintains and strengthens the modern welfare state

Surveillance in the contemporary world was first facilitated and then enabled by the introduction of identification systems. In fact, ID cards may now be considered the cornerstone of maintaining the modern state (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 3). The development of the modern welfare state is itself dependent on data collection and information gathering. Thus, the state's system has relentlessly probed into citizens' private lives to maintain itself (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 4). The ongoing gathering of state information is a decisive step toward modernity.

Similarly, the developments in information technology that have enhanced data storage capabilities further enable governments to monitor populations with much more ease than ever before (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 4). Naturally, the ease with which states can now monitor populations is likely to lead to more detailed surveillance, married with the ongoing advances in smart technologies like Artificial Intelligence that works to predict and mimic human behaviour. The registered system of identification allows states to be able first to become "modern" but also to identify, classify and monitor their citizens. Therefore, they have been considered to form part of the broad international trend toward increasing surveillance tactics (Boersma, Van Brakel, Fonion

and Wagenaar, 2014: 4). The following section will discuss how surveillance tactics like contact tracing measures have been used in the world today.

Despite the perceived liberating potentials of social media networks and digital technologies, particularly in the realm of political protesting in the 21st century, a strong sense of state surveillance continues to persist. In recent years, protestors and political activists realized the potential behind social media activism and the strength of its algorithmic nature to help advance liberation struggles, particularly under repressive regimes. In places like Hong Kong and Egypt, young people were monumental in challenging the standing political regimes and bringing about change through online protesting to garner international solidarity while using contact tracing technologies to communicate and coordinate protests that could subvert government tracking and censorship. Above all, however, contact tracing as an extension of state surveillance has reared its ugly head, raising critical international concern for the potential limiting of human rights, freedoms and prerogatives to privacy.

In quick pursuit, authoritarian inclined or surveillance states have begun using the very same tactics to further their agenda (Herrera, 2015: 354). For example, in Egypt, the Arab Spring essentially exploded the use of social media to advance political activism and protest coordination under an authoritarian regime. It finally provided a platform for disenfranchised citizens to subvert the surveillance they were subjected to work toward an emancipated society (Herrera, 2015: 354). Facebook and Twitter were now vehicles for expressing political opinion and advancing a revolution both online and offline that the world could watch happening and support it in real-time. However, these same means were turned on themselves and used by states and other citizens to lurk, troll, and report other citizens for acts of digital citizen vigilantism (Herrera, 2015: 355).

Less than four years after the Arab Spring, however, Egypt's populist military regime used these very same tactics to advance the agendas of surveillance, polarisation, and counterrevolution (Herrera, 2015: 355). In particular, the regime under Adl al-Fatah al-Sisi is extensively focused on the potential of digital surveillance, having realised the

incredible power behind it (Herrera, 2015: 355). Thus in 2014, Egypt's Ministry of Interior (MOI) announced the creation of the country's "Social Networks Security Hazard Monitoring Operation", framed as a savings measure to monitor and operate as a "public opinion measurement system" (Herrera, 2015: 355). It was further described as a security tactic to protect Egypt from those wanting to get involved in "debauchery", "homosexual acts", and to "track conversations of Islamists" (Herrera, 2015: 355). Ultimately, post-revolution, the government allowed itself sweeping powers to digitally spy on all of its internet users despite a given time frame, a necessity, or a judicial order. Legitimate concerns arise because this software has been outsourced from a private company, Systems Engineering Egypt, which has a sister company linked to it based in the United States named Blue Coat (Herrera, 2015: 355). The companies use techniques through programs that enable inspecting technologies to monitor geolocation, tracking, and extensive monitoring of one's internet search history (Herrera, 2015: 355).

Similarly, the fundamental logic of contact tracing was the same tactic used by Hong Kong protestors in the Umbrella movement to communicate using Bluetooth as an alternative to wireless or cellular networks that could potentially be followed or shut down by authorities (Stevens and Haines, 2020: 526). Moreover, the Hong Kong protestors have discovered ways and means to create peer-to-peer networks which do not need to rely on Wi-Fi or a cellular network to sustain communication. Governments are now drawing on such democratising technologies to develop surveillance technologies and encourage lateral peer-to-peer surveillance (Stevens and Haines, 2020: 526). Surveillance is detrimental for community solidarity as low levels of trust create a sense of fear and unease amongst citizens. The COVID-19 pandemic is potentially yielding a similar result.

It has also created an environment where people have become generally fearful and untrusting, a dangerous space in which conspiracy can grow. In democracies mainly, there is a sense of fear and distrust surrounding state leaders and the potential for these leaders to turn to authoritarian forms of rule at a time where emergency rules and laws are adopted (Stevens and Haines, 2020: 529). Contact tracing technologies and vaccine mandates are being employed in a global state of emergency, creating more fear and

distrust surrounding the true efficacy and the potential agendas and dangers behind such campaigns. As this plays out, citizens are essentially losing their grip on their sense of freedom and independence from the state as surveillance tactics proliferate.

Moreover, despite the perceived liberating potentials that technology has provided, the internet still relies on a fundamentally physical infrastructure that provides the authorities, governments, and telecommunications companies with fundamental control opportunities (Mare, 2020: 4245). Thus, the dynamics as mentioned above highlight to some extent the threat that the online sphere poses to the legitimacy of governmental regimes, but more importantly, the elusive and shifting nature of power that it gives the citizens who use it. While the digital sphere is often so highly praised, one should look at how it can also become a tool or an extension of government power, authoritarianism and surveillance.

2.5. The chilling effect: losing privacy and freedom to digital surveillance

The ongoing development of such technologies gives rise to the surveillance state system, characterised by an ongoing increase in surveillance and observation of its people, involving different methods of observing and documenting people's behaviour (Dencik, Hintz, and Cable, 2019: 168). Naturally, awareness around the issue has created fear around the potential of constant monitoring. A "chilling effect" may occur as people begin to fear authorities and the state in challenging institutions of power or in promoting social change (Dencik, Hintz and Cable, 2019: 168). Individuals hold back their right to free speech, ultimately changing their behaviour on the whole due to the awareness of surveillance and the subsequent need to conform to societal norms and expectations (Manokha, 2018: 228).

The "chilling effect" is a known symptom of life under a surveillance state. It occurs as individuals live in fear of engaging in certain activities because of the potential implications or consequences that may be faced if they are monitored by the state (Murray and Fussey, 2019: 44). Therefore, this chilling effect is threatening a host of human rights and, in turn, the very functioning of an effective participatory democracy. One's freedom of

expression, assembly, and association are all compromised when a chilling effect occurs, and one fears or is restricted to accessing information or engaging in communication (Murray and Fussey, 2019: 44). The chilling effect is closely tied to what Foucault initially conceptualised as the panoptic effect, demonstrating how governmentality can direct citizen behaviour.

Similarly, the development of surveillance through technological means leaves a permanent digital trace of private information that could be used to an individual's disfavour at any point in time. This creates a great sense of fear and concern whereby one begins to practice self-discipline and restraint as a consequence (Manokha, 2018: 228). When an individual fears the response of the state concerning their choice of expression, the freedom and ability to oppose or challenge state policy is therefore undermined (Murray and Fussey, 2019: 51). Democracy relies upon an informed, individualistic citizenry who challenges the existing system and feeds a free capitalist marketplace (Murray and Fussey, 2019: 44). At the same time, those who are most likely to be vulnerable to chilling effects are those who oppose or question government policy. Naturally, these citizens form part of minority groups that challenge the existing status quo with a limited set of resources (Murray and Fussey, 2019: 51). Consequently, the chilling effect of surveillance is also reproducing marginalisation while undermining the very core values of a democratic society. Surveillance efforts are fundamentally changing the existing power dynamic between the state and its citizens.

This reality is worsening today as contact tracing and personal data collection to advance digital population surveillance are measures that are being employed across multiple different regimes and contexts throughout the world. They are raising concerns around surveillance and control over personal data and giving rise to new forms of civic behaviour. Contact tracing sciences have raised concerns about how they may be abused in less liberal contexts. The use of such measures is changing the society in which they operate. One is brought to question what the future of surveillance may look like, considering that some of the most recent and significant examples of state surveillance could change the calibre of surveillance entirely.

For example, emergency savings and security measures adopted in the name of the "war on terror" following the September 11 attacks on the United States have changed the world forever. The uncertainty created a political climate in which quick decisions were made and justified, allowing the sweeping state powers to closely monitor the population (Dencik, Hintz and Cable, 2019: 168). Ever since, surveillance measures in public places have been introduced and accepted in the name of safety and security, continuing to develop rapidly. They have become the norm. At this point, however, it must be acknowledged that while the calibre of surveillance changed significantly, the process of systematic collection and monitoring of citizen data had begun long before the 2001 attacks (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 2).

While state surveillance creates a sense of social suspicion, contact tracing measures create a distrusting, fearful and fragmented society. Essentially, government encouragement to download contact tracing apps is associated with a sense of good behaviour or communal citizenship. Those who do not cooperate are often considered uncooperative and selfish or, ultimately, bad citizens. Therefore, citizens are likely to fall victim to social pressure, encouraging them to cooperate with the state's new surveillance measures. This forms part of Foucault's theory of governmentality and the state's power to direct people's behaviour without necessarily needing to apply force. Ultimately, one may argue that the surveillance technologies being developed to contain the COVID-19 pandemic threaten the functioning of participatory democracy in several ways. There is a lack of critical analysis and questioning around measures adopted under the name of political savings measures.

2.6. Technological developments behind surveillance today

The heights that surveillance can reach have developed with the rise of modernity, technology, and the centralised bureaucratic state (Manokha, 2018: 226). Surveillance has become an essential element for the upkeep of capitalist society and industry as it forms part of its four institutional clusterings, namely, capitalistic enterprise, industrial

production, centralised control over the means of violence and, of course, surveillance (Manokha, 2018: 226). Technological advancements have also made storing and organising data so accessible that more advancements continue to be made in profiling, scoring, categorising, and recognising data associated with specific individuals. Machine learning algorithms are used to explore patterns that can reveal invaluable information about the behaviours of users as well as groups of users and their collective behaviours (Fahey and Hino, 2020: 3).

At this point, it is important to acknowledge, discuss and to make abundantly clear that this study recognises and appreciates many aspects of technology and surveillance technologies in today's world. Surveillance as an initial reaction to safety and security, as a war on terror, has, in many ways, improved and saved lives. It has created less space for acts of unsolicited violence to occur, and in turn, has protected innocent civilians. This study is also supportive of the belief that surveillance and police can have a positive influence society in the sense that their presence helps to prevent crimes from being committed. However, the presence of police and surveillance should not be synonymous with a police nor a surveillance state.

The rise of surveillance capitalism that has also led to an understanding of how powerful human behavioral data is, with this, there has been an unprecedented rise in technologies that have been able to significantly improve the ease of daily human life. Artificially intelligent machines and technologies have taken over processes and services typically undertaken by humans, in a more efficient way than ever before. This has afforded society with more time to focus on matters that take higher priority, whether it be to spend more time with one's family, on one's job, or to simply stray from doing tasks that can be sufficiently completed with the help of computer technology.

What is more, I tend to disagree with the widely renowned Shoshana Zuboff (2019), who argues that the boom of technologies has led society away from information equality. In fact, one might argue that the ease of accessing information has somewhat leveled out the playing field. Wider accessibility to the internet obviates the need for schools or

universities to exist as physical and structural entities. This may, in turn, see a societal shift away from the popularity of financially exclusive and colonial institutions of education and higher education.

However, as society shifts life more and more to the online sphere, the rise of surveillance potentiality likens. When paired with the rise in social media networks, data has become a liquid commodity traded between private and governmental bodies, blurring the common conception of who may be doing the online surveillance (Manokha, 2018: 227). In addition to this, the very omnipresence of digital and social platforms that are amassing their databases are encouraging more and more actors to either do the same, to buy, or to get access to these databases for the sake of their profit-making endeavours (Manokha, 2018: 228). Today, the value of ICT companies like Facebook or Amazon lies in their access to massive databases on their users and customers (Fahey and Hino, 2020: 3).

Communication technologies have created a perfect panoptic setting in which constant surveillance is taking place. To add to this, there is a growing value attached to personal data and transnational corporation capitalisation on such data, exposing new forms of capitalism. The term transnational in this instance indicates the economic side of things and its relative social, political and cultural processes. These include class formations that "supersede the nation-states" (Robinson and Harris, 2000: 16). Transnational corporations came to prominence in the 1980s and have since dominated the world economy, forcing economic and political restructuring based on the fundamental value of market liberalisation (Robinson and Harris, 2000: 29).

Transnational corporations control the global economy through multilateral and national institutions, among the likes of the International Monetary Fund, the World Bank and the World Trade Organization (Robinson and Harris, 2000: 40). They play an important role in creating dynamic power relations and shifts within the processes of social production that contribute to the ever-shifting class structures (Robinson and Harris, 2000: 16).

Moreover, these bodies that have just been described as some of the most influential organisations in controlling the global economy are the same bodies relying on and trading in access to volumes of personal citizen data.

The constant development of digital communication technologies and the importance of data, including common computing systems and cloud storage systems, are all essentially giving rise to a new form of social ordering referred to as algorithmic regulation (Yeung, 2018: 505). There is a common conception that algorithms can be harnessed to find solutions and perform functions for political and social policies that people may struggle with. They are "encoded procedures for solving a problem by transforming input data into the desired output" (Yeung, 2018: 505). The definition and understanding of an algorithm differ according to the field in which it is used and understood. For social scientists, the term is used to understand the greater "sociotechnical assemblage", which includes algorithms, the computational networks that the algorithms make use of, the people behind the making and designing of the algorithms, the data or people that the algorithms make use of, as well as the very institutions which provide the services (Yeung, 2018: 506). Social scientists then look at the broader social endeavour that this is all connected to, which together constitutes a network of authoritative systems for knowledge production (Yeung, 2018: 506).

This broader social endeavour of surveillance has resulted in decreased individual research and decreased expression of opinions that differ from the dialogue of saving congruent with the state agenda. An awareness around increasing surveillance measures has resulted in significant decreases in online searches that may be security-sensitive (Manokha, 2018: 229). In addition, significant scores of adult internet users reported that they would refrain from engaging in certain dialogues online that could risk getting them into trouble with the government (Manokha, 2018: 229). This above-mentioned chilling effect extends beyond online action, whereby social media users restrict themselves or refrain from engaging in certain activities to avoid their actions being documented online (Manokha, 2018: 229). Therefore, if citizens refrain from or are afraid to take part in contentious action, the democratic system is at stake. Surveillance measures are thus

constantly changing the shape of the world as different power dynamics change and emerge. With the rise in big tech and the global acknowledgement of the power behind data, government regimes have become increasingly reliant upon digital infrastructures and privately-owned companies (Dencik, Hintz and Cable, 2019: 170).

These regimes run according to the logic of surveillance capitalism, using and collecting personal information by extracting, monitoring, personalising, experimenting and predicting based on ongoing readings of one's online transactions (Dencik, Hintz and Cable, 2019: 170). Surveillance capitalism is fundamentally similar to industrial capitalism, however the system of surveillance capitalism profits from the collection and analysis of human behavioral data. Whereas the system of industrial capitalism profits from the exploitation of natural and human resources. The potential of this massive reservoir of behavioral data that has existed for years, but has primarily been used within businesses for the improvement of internal analytics (Zuboff, 2019: 10). Under the system of surveillance capitalism, however, this bank of data has been realized, and businesses sell masses of data to other businesses that can benefit hugely from millions of people's private information.

As these infrastructures become more naturalised, academics refer to the politics of a "post-digital" world where activists are increasingly concerned with the ways the networks are built around the centres of power and how these need to be challenged in order to achieve any kind of genuine social emancipation (Dencik, Hintz and Cable, 2019: 170).

2.7. A new world order under surveillance capitalism

Public awareness of the scale and potential of data collection and use in today's digital interactions and transactions significantly impact social and political activists. Monitoring and recording people's movements threaten and limit the potentiality of dissent and protest to certain degrees (Dencik, Hintz and Cable, 2019: 183). Whether the limiting of protest is a deliberate choice this impacts the dynamic of governance by enfranchising those already in power while simultaneously disenfranchising others. Naturally, this will

further impact social, economic, and political agendas (Dencik, Hintz and Cable, 2019: 183). Autonomous communication and dissent are therefore stifled by this surveillant political economy which demands the call for social justice and more focus on the issue of data justice. This calls for genuine concern for human rights and the function of participatory democracy (Murray and Fussey, 2019: 32).

The understanding that the internet can be both a tool of emancipation and a facilitator of totalitarianism is not new. However, the understanding of the extent to which one's personal data may be used for both economic and political gain is more recent for people throughout the world. Surveillance potentialities that contact tracing may be opening the door to are proliferating existing concerns for the implication of one's data privacy and protection, as well as one's human rights in the context of liberal democracy (Guild, 2019: 268).

The abundance of technologies used in daily life that can capture personal electronic communications has created a reality in which one's rights and obligations are no longer exclusively tied to the state (Guild, 2019: 269). Daily communications and the transference of personal data happen transnationally and internationally, and these cannot necessarily be controlled by national law. Nor can the national law protecting privacy in one country be expected to be the same as those in another country (Guild, 2019: 269). This creates a loophole for transnational companies that seek big data collection to benefit their performance, often an intrusive automated performance. This also creates room for human rights laws to be defined around bulk communication monitoring. It ought to consider the extent of information revealed by communications data and the true extent to which surveillance is taking place.

It has become increasingly clear that the commodification of one's data contributes to the profitability of companies while it threatens to undermine personal autonomy and democracy. Shoshana Zuboff (2019) has been central in her research and vocalisation on the issue of what has been deemed the issue of surveillance capitalism. Its key defining features are the ongoing exploitation of multiple data sources defined by a lack

of structural responsibility or mutually beneficial relationship through the process of data extraction. Under a system of surveillance capitalism, internet users have no autonomy over their data when using internet platforms. Lastly, it entails using analytics and its production of anticipatory conformity (Lyon, 2019: 68).

Surveillance capitalism is a term used to describe how everyday communication between people is used to sustain a highly monitored society. Ordinary people and internet users provide data, whether wittingly or not, which is then quantified and organised to track people in real-time. The way this information system is built characterises a system of governance that capitalises on a type of political economy that uses this data to predict and modify citizens' behaviour to produce revenue and market control (Dencik, Hintz and Cable, 2019: 167). In the world of COVID-19, where life has become more physically insular, living and working from home while socially distancing, people rely on an online sphere to maintain both a work and social life. This provides tech companies and governments alike a chance to capitalise on these everyday communications to maintain surveillance levels. Similarly, contact tracing technologies essentially provide a chance for states to enrol citizens into a much more precise and intense surveillance tracking system.

Under the system of surveillance capitalism, data is a raw material used across digital platforms that generate huge profits out of the invasion of one's privacy through the ongoing collection of personal data (Manokha, 2018: 231). Moreover, the system of surveillance capitalism which is currently being sustained by the encouragement of contact tracing technologies, is essentially dominated by the role of biopower as a politics that depends upon the power over life. This phenomenon occurs as there is no single collector of data or one sole subject watching over people. Surveillance today is more omnipresent than ever with the advances in surveillance technologies and the awareness around data monopoly's value and potential economic success.

In fact, according to the United States' Defense Innovation Board (2017), data should be regarded as the 21st century's equivalent of a global natural resource (Tréguer, 2018:

146). Data is helpful for military innovation as its value can be used to advance computing technologies that work to reveal insights and predict people, companies, and states' intentions and capabilities. At the end of the day, one's data becomes the raw material used to identify patterns and the exceptions to these patterns used to create machine learning systems (Tréguer, 2018: 146). This forms part of a greater fight for technological superiority amongst world superpowers who are ultimately fighting to amass the most data.

This is where big tech companies come into play, as they work alongside government executives, selling solutions to improve their technological advances and help improve security bureaucracies (Tréguer, 2018: 146). Herrera (2015: 355) highlights in her work how the "techno-evangelists" were only correct to a certain degree in their belief in the unparalleled powers of technology to open communication and information and consequently transform the world into a free and open place. However, technology alone does not create a free nor a more open society. Authoritarian governments may have liberalised their economies as well as their media and communication sectors, yet they did not hold back on their surveillance tactics (Herrera, 2015: 355). As a matter of fact, neither have liberal democracies.

At this point, it is essential to discuss the restructuring and the transformation of the global economy due to digitisation. Information technology has been the greatest driver behind state surveillance (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 4). It has enabled the mass movement, storage, and organisation of data in technologically mediated worlds, giving states unprecedented penetration opportunities (Boersma, Van Brakel, Fonion and Wagenaar, 2014: 4). Together with states, the global surveillance capitalism system depends on the daily usage of the Internet of Things (IoT) and its many daily technologies that maintain everyday surveillance. The dominant political economy is underpinned by this system, shifting away from the need for geopolitics to gain power within the world system.

Added to this, the adaptations that have been forced onto society and the economy by the novel COVID-19 coronavirus pandemic have only sped up the process. The process in which the global tech giants are amassing more power than ever before through a new bloc of transnational capital that controls the entire global economy (Robinson, 2020: 3). The problem here is that the already unequally distributed and highly concentrated global capital will be further entrenched, worsening inequality and increasing international tension (Robinson, 2020: 3). Digital technologies may arguably be considered a symptom of an impact of the coronavirus pandemic as it contributes to a large assemblage of already existing social inequalities (Madianou, 2020: 3). As of October 2020, it is estimated that around 60% of the world's population is active on the internet (Johnson, 2021). Of this population, there is a heavy dependence and belief that the internet is a tool to express and uphold the values of democracy and human rights. With the ongoing data collection and increasing power of global tech corporations, existing power dynamics will continue to be deeper entrenched should they not be challenged enough.

Nevertheless, Robinson (2020: 4) speaks of a growing post-pandemic capitalist paradigm that is based upon the digitalisation and application of what is referred to as the fourth industrial revolution technologies. This essentially refers to the development and use of artificial intelligence, which includes machine learning, biotechnology and the Internet Of Things (IoT). The normalisation of mass collection and data storage are characteristic of these technologies (Robinson, 2020: 4). The looming post-pandemic capitalist paradigm is likely to contribute to the further limiting of one's privacy and general freedoms under the system of democracy. Thus, the idea that one is free under a liberal democracy almost loses its meaning entirely. Surveillance tactics are and have been in full swing throughout history. However, the heights that surveillance is reaching have grown exponentially with the swift digitisation of life through forced adaption due to the novel COVID-19 coronavirus pandemic.

Castells' (2009: 402) rich contribution to analysing the nation state's loss of sovereignty bears relevance to this very conversation. It has been known that democracy has been in a state of crisis for the past century. At the same time, the dynamics of global flows of

networks and transnational capitals that underpin society today are simply unparalleled to any other time in history. For Castells (2009: 402), both the nation-state and the citizen have lost most of their sovereignty to the networked society that is run by flows of wealth, information, and power. According to Castells (2010), the network society characterises the entirety of the world today. The network society functions upon the global economy that may be understood by:

"The almost instantaneous flow and exchange of information, capital, and cultural communication. These flow order and condition both consumption and production. The networks themselves reflect and create distinctive cultures. Both the networks themselves and the traffic they carry are largely outside national regulation. Our dependence on the new modes of informational flow gives to those in a position to control the enormous power to control us. The main political arena is now the media, and the media are not politically answerable" (Castells, 2010: 1).

Essentially, life in the information age is both dominated and controlled by networks. These networks control how society operates. According to Castells (2010: 500), the "diffusion of networking logic substantially modifies the operation and outcomes in processes of production, experience, power and culture". He further argues that the most significant contributing factor to the state's loss of legitimacy and the overall crisis is the fact that it has been unable to execute its duties as a welfare state (Castells, 2009: 402). This has been a consequence of the internationally interdependent system of production and consumption and how this has forced shifts in the capitalist system (Castells, 2009: 402). Today's network society has created political participation and social demands that the system of democracy cannot keep up with. The system fails to help ordinary citizens address the problems they encounter in daily life (Castells, 2009: 413). As the modern state is further fragmented, the democratic system is losing relevance and meaning.

While the COVID-19 health pandemic has made the argument clearer than ever that the internet is a lifeline, the COVID-19 novel coronavirus pandemic is also the first global health pandemic to happen in the time of the information age (Fahey and Hino, 2020: 1).

Technological devices with surveillance potentialities are more popular than ever before as people work from home and use mobile devices with contact tracing apps. With the mandating of different COVID-19 protocols within countries, people have become increasingly aware that there is a possibility of being watched or tracked by different government surveillance measures. People are also aware that citizens alike are policing one another to follow government protocol. Similarly, the state relies on this process whereby the populace police one another. Surveillance has brought about the proliferation in lateral or peer-to-peer surveillance, which results in self-censorship due to the concern for what one's online peers may think or how they may respond (Manokha, 2018: 229). The notion that discipline is laterally enforced from peer-to-peer can be explained by and forms part of Foucault's theory of biopower which is put into place by governmentality.

Surveillance is a popular measure used by states to control and monitor the population throughout history. The COVID-19 pandemic, however, has provided a unique circumstance for public health surveillance through the use of contact tracing measures. Being the first global health pandemic to take place in today's information age, the available technologies enabling the digitisation of surveillance are simply unparalleled to any time in history. Surveillance in public health, married with the longstanding debates between collective interest and individual rights, forms part of a considerably large debate in reducing online privacy and data commodification.

Therefore, this provides an interesting and important topic of debate concerning the implications for human rights and the long-time coming failure of democracy. Increasing trends in surveillance and data commodification, as mentioned above, contribute to the development and strengthening of the surveillance state that runs according to the logic of surveillance capitalism. While surveillance does serve a purpose in controlled environments, it has notoriously undermined human rights and, subsequently, democracy. Contact tracing measures and public health emergencies have historically resulted in the discrimination of minority groups and the deepening of already existing inequalities. A culmination of contributing factors has created a fearful society when public

trust and solidarity are most needed. Strict public policy and protocol thus ought to be put in place to prevent such irreparable damage to human freedom in the future of the novel COVID-19 coronavirus pandemic.

3. New forms of digital health surveillance during COVID-19

3.1. Introducing contact tracing applications

The COVID-19 crisis has been an interesting space of study and analysis, having happened congruently to a digital revolution. It has been a time in history that citizens have celebrated and feared the impacts of the rapid advances in digital technologies. What is commonly known as public health surveillance is the systematic collection, storage, use and dissemination of one's data to identify and contain the spread of an epidemic (Sekalala, Dagrón, Forman and Meier, 2020: 7). This is made possible through contact tracing apps and social media platforms on one's mobile phone device. While digital surveillance tools are critical savings technologies during the global health pandemic, they have also raised a host of questions around the commodification of one's personal health data and what this may mean when the pandemic has subsided.

Understandably, there is rising concern regarding this power that states harness to develop accurate and detailed contact tracing technologies. The COVID-19 pandemic has proliferated a worldwide panic to adopt emergency savings responses to help contain the spread of the virus as quickly as possible. However, under the guise of saving, some may argue that the COVID-19 may be providing states with a window in which they are simply capitalising on expanding surveillance measures.

This chapter will look at the efficacy and the human rights implications of contact tracing measures, assessing what they may ultimately mean for the state of democracy and global capitalism. At large, there is fear that the increase in surveillance tactics through public health technology, namely contact tracing applications, may lead to an abuse of power. Previous historical moments have demonstrated how health or security crises have been used to expand surveillance and ultimately state control. Additionally, the awareness of surveillance, married with the unknown of the novel COVID-19 coronavirus pandemic, are creating an environment of distrust and fear. Contact tracing technologies also create global digital divides between those who do not have device access and those

that do. Naturally, notions of distrust and fear create fragmentation within society, contributing to a weak democratic base.

Biopower as regulatory power will be used as a way to explain how the COVID-19 pandemic has exposed the state's fundamental reliance on the policing of human bodies. Biopower is 'a power that exerts a positive influence on life, that endeavours to administer, optimise, and multiply it, subjecting it to precise controls and comprehensive regulations' (Kalpokas, 2020). Therefore, this study will expand on Foucault's argument that society's greatest threat is a deviation from the dominant account of human biology and its relation to optimal economic productivity (Kalpokas, 2020). Typically, biopower may benefit society through different biopolitics that have enforced mandatory medical checks, tests, and vaccinations. Foucault's theory of governmentality will also be employed to explain the ways in which the state relies on its citizenry to govern one another through policing. Moreover, this chapter will demonstrate how the role of governmentality in the time of COVID-19 contributes to the more general state surveillance.

The COVID-19 pandemic has exposed a sinister side of biopower. The pandemic has uncovered an intrusive and controlling biopolitical world system that continues to use and develop unprecedented and unanticipated surveillance tactics (Kalpokas, 2020). Technology is constantly developing, and with this, so too does surveillance. Moreover, the COVID-19 pandemic has laid bare the reality of the grip of power that the state has over the human biology. This is problematic for the meaning of democracy and the direction in which it is currently headed. As a part of the bigger system of state surveillance and surveillance capitalism that characterise life today, contact tracing measures have been a key area of debate in response to the COVID-19 pandemic. Contact tracing in the time of the COVID-19 pandemic forms part of a critical debate that Zuboff (2019) articulated concerning the dangers behind the lure of technological "solutionism" and the ongoing advancement in surveillance technologies.

The pandemic at large has raised concern for the ways that it is impacting and threatening the legitimacy of democracies throughout the world. Emergency public health responses

have, in many instances, been abused. Interestingly, there has not been a clear pattern between the abuse of power and the type of regime in which it has occurred.

3.2. How contact tracing applications work

In an attempt to contain the spread of the coronavirus, contact tracing is a measure adopted to identify and monitor those who may have been infected. By collecting necessary relevant information about those who have been infected, contact tracing aims to recognise and monitor who the infected individual may have come into contact with (Idrees, Nowostawski & Jameel, 2020). Public health surveillance in the COVID-19 health pandemic has popularised a new form of digitised contact tracing. Contact tracing applications enrol citizens into a “state-linked infrastructure of viral tracking and knowledge production” (Stevens and Haines, 2020: 525).

Contact tracing in the time of COVID-19 has been a process of leveraging digital and daily technologies and maximising the fact that most citizens in developed countries use these technologies. Smartphones and watches contain GPS chips and Bluetooth radios that make exact location tracking possible (Fahey and Hino, 2020: 2). Thus, digital contact tracing efforts have been made possible by turning people’s smartphones into contact tracing devices. A contact tracing app makes use of the user’s smartphone as a device that essentially becomes a sensor of the coronavirus as it infects different people. As soon as an individual is diagnosed with the virus, the government initiates the contact tracing process. This is done by collecting data from the relevant patient’s phone, then centralising and redistributing the data (Stevens and Haines, 2020: 525). This network is only enabled by the government in control. In other words, the app uses Bluetooth technology to store data about other smartphones that may have come into contact with or close proximity to one’s own smartphone (Stevens and Haines, 2020: 524).

Savings technologies like the vaccine passport and contact tracing apps have been developed to facilitate the resumption of daily functioning life, work, and travel. They are adopted for the sake of national security and, ultimately, what these above-mentioned

concerns are all underpinned by, the national economy. Essentially, the health and medical profile of an individual will therefore determine their right to cross-border travel and freedom of movement for the sake of preserving the national economy. At the same time, by allowing 'essential services' to continue operating during the height of the COVID-19 pandemic, governments were then able to decide which bodies were worth putting at risk for the sake of economic growth, which was also framed to be for the benefit of the community (Dias and Deluchey, 2020: 8).

The COVID-19 has played an important role in laying bare the realities of today's world system controlled by biopolitics. More so, society is quite clearly organised by a hierarchy of disposable bodies. The control over these bodies is utmost important for the regulation of power and ultimately, the global capitalist economy. In fact, Agathangelou (2013: 467) summed this up succinctly in lamenting how capital regimes always "require new forms of subjugation".

3.3. Distinguishing safe and unsafe bodies through contact tracing technologies

An ongoing collection of data has been considered to be a powerful step toward modernity. This study will unpack these logics of the state that, according to Agathangelou (2008: 128), "rouse desire to 'explicitly and simultaneously link the imperial project to militarisation and nation building.' In this production, a certain mooring of desire and the production and mobilisation of pleasure is summoned up in the affective calling toward 'enemy production.'" Alexander (2005) expands on the production of the enemy through nation building which can be understood as "a form of hypernationalism with constituent parts: the manufacture of an outside enemy to rationalise military intervention, and secure the annexation of lands; the production of an internal enemy to rationalise criminalisation and incarceration" (Agathangelou, 2008: 127).

The creation of the enemy naturally produces the need and desire for safety, in turn, justifying the saving of certain bodies over others. More so, by making some groups

believe that the state is looking after them, they are drawn into believing that the state promises an end to marginalisation and that they hold a place as legitimate subjects within the system of global capitalist democracy (Agathangelou, 2008: 128). This understanding, therefore, helps make sense of the widespread adoption of technologies of the state that are probing into private life, aiding the gathering of information to contribute to state development.

Contact tracing has taken different forms across different government regimes across the world. Interestingly, levels of political freedom have not always directly correlated to a country's pandemic response, as one may have assumed. There is, however, an overall trend that existing democracies face the threat of eroding and that established authoritarian regimes are being strengthened. Although, one cannot look at the emergency responses of the COVID-19 pandemic in isolation. A longstanding history of surveillance and its development with the rise in digitisation has contributed to the worldwide trend of the decline of both democracy and capitalism.

The COVID-19 pandemic requires the strict monitoring of individual health data, further proliferating the notion of the already existing surveillance state. After all, the swiftness with which such savings measures have been adopted suggests that there has not been ample time to consider the potential human rights implications, nor has appropriate policy been developed to control the regulation (Wilford et al., 2021: 393). Inequities in access to the vaccine, limited vaccine production in certain regions, personal medical concerns and bodily autonomy concerning vaccine-hesitancy for a host of personal reasons, as well as data privacy concerns related to the passport are all very serious and potentially life-changing factors that savings measures like the vaccine passport does not consider.

Should it remain unchecked, the contact tracing technologies will normalise a world that is divided by "safe" and "unsafe" bodies (Wilford et al., 2021: 394). Ultimately, the pandemic is creating a world that accepts the securitisation of the human body whereby bodily risk will determine subjection (Kalpokas, 2020). The consequence of this is therefore a means of democratic repression.

What is more, there is a lack of critical analysis and questioning surrounding the ethical and regulatory processes of the networks used to develop surveillance technologies like the vaccine passport (Wilford et al., 2021: 394). Developing such technologies involve a plethora of integrated networks that connect institutional actors with cutting-edge technologies. Within this environment, where technologies like contact tracing applications and vaccine passports are developed by a collaboration of tech companies and open-source communities, regulation is notoriously weak, and risks are high (Wilford et al., 2021: 394). This forms part of the networked society that both nation states and citizens have lost their sovereignty to in a tireless pursuit for modernity. With a bigger goal in mind, the main pursuit of modernity tends to dismiss critical human rights concerns as it probes into private life.

3.4. Regulatory gaps in contact tracing technologies

In a study done by the United Kingdom's National Health Service (NHS), the introduction of the Digital Technology Assessment Criteria was used to assess the risk of global digital health applications at the beginning of 2021 (Wilford et al., 2021: 394). The overriding outcome was that there is yet to be a contact tracing application that does not have an element of serious privacy infringement in one way or another.

Significant standing gaps in regulation and policy exist, which are contributing to their current inefficacy. These include, and are not limited to, several problems complying with the General Data Protection Regulation (GDPR) (Wilford et al., 2021: 397). The GDPR hold the responsibility to: inform individuals when their data is gathered and processed, delete data that no longer needs to be kept, or an individual withdraws their consent over personal data retention (Idrees, Nowostawski & Jameel, 2020). The GDPR also grants the right to object the processing of personal data. As it stands, the strategy of contact tracing in the face of COVID-19 is to track the movement of the carrier of the virus and in turn, does not prioritise nor protect the privacy of app users (Idrees, Nowostawski & Jameel, 2020).

Issues concerning transparency as well as commercial interests may create regulatory barriers to the true effectiveness of contact tracing applications and vaccine passports (Wilford et al., 2021: 398). The current gaps in understanding of the nature of the virus itself also brings one to question the introduction of contact tracing. While contact tracing may aid the process of containing the virus, it is rendered redundant where the COVID-19 virus is spread through the air. In these cases, the virus can spread without direct contact between humans. What is more, due to the limited research on the virus as a result of its mere infancy, the variety of symptoms make the source of contamination difficult to trace (Idrees, Nowostawski & Jameel, 2020).

This leads one to question the ethics behind savings measures if contact tracing applications are being adopted with such blatant shortfalls. Similarly, the primary technology platforms employed to develop contact tracing applications have not been able to prove seamless regulatory measures. In a study of the three main technologies used for contact tracing throughout the world, namely: open-source, blockchain, and data networks, a rigorous analysis has demonstrated how each platform yields a different set of issues that raise concern around ethics and transparency in developing contact tracing and vaccine passport technologies that are compliant with the rules of the General Data Protection Regulation (Wilford et al., 2021: 402). The following discussion will briefly expand upon the shortcomings of the available and widely adopted technologies.

The widely adopted and trusted Blockchain is a distributed ledger technology that operates upon and promotes decentralised authority and non-regulation. Trustless by design, it allows a network to validate transactions without trusting any central authority or control (Wilford et al., 2021: 399). Where this may be of value in many circumstances, the use of blockchain technology to develop health technologies is problematic considering the thorough regulation that ought to go into developing health technologies (Wilford et al., 2021: 399). What is more, blockchain aims to support the values of self-sovereign identity and data privacy, proving another hindrance to regulating contact tracing technologies.

Similarly, IBM, a leading corporate in developing and marketing its Digital Health Pass, bases its blockchain as well as its quantum computing services upon the open-source (Wilford et al., 2021: 400). Through the use of such technologies and the open-source nature of the like, companies like IBM market digital vaccine passports to be “open”, “trustworthy”, and “transparent”. However, Wilford et al. (2021: 400) highlight how complex the topic of transparency is. Although the nature of blockchain is open or free to some degree, there is no guarantee that the open-source nature of blockchain development is equal to the transparent implementation of a specific blockchain (Wilford et al., 2021: 400). Similarly, open-source software creates concerns for accountability due to its decentralised nature and the role of collaborative communities (Wilford et al., 2021: 401).

The data networks that are drawn from to realise the creation of digital contact tracing technologies will require various centralised and decentralised sources to be able to create individual personal profiles that represent one’s COVID-19 health status (Wilford et al., 2021: 401). Consequently, not only will this profile contain an individual’s contact tracing and vaccination details, but it will expose or highlight the entire health status and history of an individual (Wilford et al., 2021: 401). The potentiality of serious privacy breaches lie ahead should the creation of vaccine passports like the above-mentioned IBM Digital Health Pass be actioned. Should the combination of artificial intelligence (AI), blockchain and the Internet of Things (IoT) be used to create such technologies, a mass of interconnected systems and data will together create a fluid system that is difficult to regulate in terms of ethics and ultimately, more policy vacuums and regulatory gaps (Wilford et al., 2021: 401).

Unfortunately, the reality of implementing a contact tracing application or a digital vaccine passport will require a range of actors, including different data sources and authorities, that will together create an extensive network of resources that the application may pull from (Wilford et al., 2021: 402). Thus, there cannot be a central authority over the

passport. Moreover, multiple institutions will have access to the available data that is also vulnerable to hacking (Wilford et al., 2021: 402).

Technically speaking, contact tracing applications have not yet been mastered nor do they align with transparent democratic principles. Nevertheless, there is a significant amount of citizen participation and collective hope that by cooperating with the state, the COVID-19 pandemic will be brought under control. Ultimately, a great majority are willingly taking part in an invasive form of state surveillance based on the belief that the state wants to protect and preserve human life. This mass cooperation is enforced by implicit coercion to be a good citizen and in turn save the lives of other citizens. Biopower as a source of societal regulation is essentially what encapsulates this idea and has been a powerful force in controlling and policing human bodies for centuries. From this perspective, contact tracing applications may be seen as another space of exclusion within society, particularly in the divisive world of COVID-19.

3.5. Contact tracing applications in practice: the case of Asia

Countries have been trying and testing different contact tracing technologies in an effort to contain the virus and limit the damage within localised environments. This study takes a particular interest in Asia's experience due to both its close proximity to the origin of the virus and its array of vastly different political regimes. Asia is an interesting space of analysis because it contains some of the world's leading democratic regimes and successful responses to the virus as well as its extreme opposites. Asia is also home to some of the world's leading autocracies. It therefore seems appropriate to begin with China due to its lead in global technology, but also because it was the first country to experience the outbreak of the virus.

China used an interwoven network of public health data, surveillance, and state police in emergency response to controlling the spread of the virus (Greitens, 2020: 172). A policy of prevention and control have been central to the People's Republic of China's (PRC) leadership both in the past and in the current handling of the COVID-19 pandemic. In fact,

prevention and control measures were also central to the country's handling of the SARS pandemic. In parts of China, citizens are monitored through a compulsory phone app and QR code that determines their access into public spaces based on infection status. The app will also alert local police if a person tries to enter a public space and they should be in quarantine (Kitchin, 2020: 363). As a result of China's relative success in containing the spread of SARS, it has expanded measures of social control and security to develop what is currently a "three-dimensional, information-based system of prevention and control for public security" (Greitens, 2020: 173). These measures, however, are by no stretch unfamiliar to China's regime. State monitoring and control through intelligent surveillance systems were well established and normalised before the outbreak of the novel COVID-19 coronavirus.

As a result, public security was able to work seamlessly alongside big tech among Tencent and Alibaba to develop the most efficient contact tracing applications. Being some of the world's biggest and most potent data-rich companies, the Chinese government have been able to develop a contact tracing app that has individual data on movement, contact, as well as biometric data like body temperature and heart rate data (Greitens, 2020: 173). The app collaborates with local and national police that amongst one another, share databases, which allow the state to be able to enforce local lockdowns where necessary (Greitens, 2020: 173). The app technology makes this possible by utilising such data to organise people according to colour codes that are used to determine who is permitted into certain public spaces and who and where people may move.

China's illiberal approach is unsurprisingly similar to its already existing state surveillance system. Being the leading world power that it is, however, there is potential that China's model of pandemic response could be diffused worldwide (Greitens, 2020: 169). As it stands, Chinese tech companies have already exported surveillance technologies to at least eighty countries throughout the world, ranging from fully liberal democracies to outright autocracies (Greitens, 2020: 177). One cannot, therefore, assume that the country's pandemic response will be in line with its political stance.

This concern has been born out of the fact that China is a leading world economic power and an industry trailblazer in the world of technology. The world's first model of the pandemic response system, therefore, is based upon that of the world's largest autocracy (Greitens, 2020: 169). Public health responses throughout the rest of the world that are borrowing technologies or using China as a model to learn from, spreading and normalising a fundamentally autocratic approach to public health. The problem is that people are not questioning or challenging the system enough. People may either assume that the state has public health in its best interest, or more likely, they are guided by biopower. Governmentality, the ability to direct citizen behaviour, has left citizens with little room to deny or challenge emergency public health responses to the COVID-19 pandemic. Consequently, the spread of illiberal practices and approaches to the COVID-19 pandemic are being accepted in the name of saving and may negatively impact democracies throughout the world.

While the instantaneous flows of information, communication and capital of the networked society have created a world in which one's rights are no longer exclusively tied to the state, the sovereignty of national law to protect its citizens has also become blurred (Guild, 2019: 269). Therefore, while the spread of China's autocratic COVID-19 emergency response poses a threat to democracy, more so should the technologies of surveillance themselves.

3.6. Approaching data privacy

The proliferation of data collection and the use of contact tracing technologies have simultaneously raised a host of issues concerning potential human rights implications and the extension of surveillance by the state. Surveillance tactics adopted in the past under emergency powers have proven to be both difficult and unlikely to roll back on. The issue of digital privacy also raises widespread debate and distrust around issues of surveillance and the threat that the issue poses to the stability and legitimacy of liberal democratic regimes. The swift adoption of political savings measures in the climate of the COVID-19

pandemic infringes on a variety of human rights. Moreover, too many limitations to the contact tracing apps exist for them to be effective as well as to align with international standards of human rights. This study will also demonstrate that how if there is no widespread adoption of contact tracing applications, they cannot operate to their full potential.

Contact tracing also requires complete transparency surrounding data collection and retention, which is lacking so far, resulting in distrust and non-compliance. In order that the technologies used are not abusing civil liberties, they ought to be; proportional, necessary, limited in time frame and scope, and they should be open to checks and balances by civil society. This next section will look at the ways that both democracy and human rights are threatened as well as the social and political pressures that individuals are put under, undermining individual autonomy over their bodily choices.

As it stands, there is an ongoing contentious debate between national governments and corporations about the best way forward for contact tracing. The greatest divide lies between a data first versus a privacy-first approach. While data first maintains the retention of tracking data and openness to authorities, privacy-first prioritises the citizen's control over their own personal data while still being able to maintain the process of contact tracing without necessarily exposing exact individual movements (Fahey and Hino, 2020: 2).

Adopting a data-first approach means that each citizen may be individually tracked by their smartphone, whereby all personal details and contact interactions may be monitored and captured on a central server (Fahey and Hino, 2020: 2). A privacy-first approach, on the other hand, makes use of dynamic identifiers that are regularly changed. In this manner, personal details like contact interactions are stored in a cryptographically secure way on their own local device, meaning that little to no data may be stored on a centralised server (Fahey and Hino, 2020: 2). Ultimately, however, both approaches perform the same function of contact tracing.

Asia has been found to contain some of the most extreme divergent approaches between data first and privacy first, making it an interesting space of analysis considering the experiences of the continent with SARS and the Middle East Respiratory Syndrome (MERS), as well as its timing of democratisation (Fahey and Hino, 2020: 3). The learning environment of pandemic response is an international system in which countries teach and learn from one another in a global epistemic community of medicine and public health (Greitens, 2020: 175). Countries learn from and teach one another their best practices and successes in containing the virus and how they may be able to employ such measures in specific local contexts without being detrimental to the democratic system (Greitens, 2020: 175). Democracies in Asia have served as successful models in their early responses to COVID-19.

While one may be tempted to assume a country's political stance or degree of political freedom as a directly correlated means to explain their approach to such contact tracing technologies, this, however, has proven to be counter-intuitive to one's assumption. In fact, the strongest data first approaches have been adopted by liberal democracies like South Korea and Taiwan, while the privacy-first approaches have been adopted by the likes of China and Qatar (Fahey and Hino, 2020: 3). As a matter of fact, Taiwan has provided the world with a model of contact tracing that least interferes with personal data retention. So far, it has best illustrated how contact tracing can be implemented by least threatening democratic principles.

3.7. How Taiwan and South Korea developed successful pandemic responses

Taiwan and South Korea, in particular, have provided the world with perceived successful models on which countries are basing their pandemic response and surveillance tactics (Greitens, 2020: 176). In fact, Israel has even based its surveillance approach on Taiwan's initial success. Interestingly, both Taiwan and South Korea have modelled pandemic response systems off previous experiences with the 2003 SARS outbreak and the 2015 MERS outbreak, respectively (Greitens, 2020: 184). What is more, both countries have had a recent history of authoritarianism that has made civil society very

aware of the potentiality of unlimited surveillance and its costs (Greitens, 2020: 185). There has therefore been a big focus on creating solutions that are compatible with a democratic system, as well as simply being prepared for a public health crisis well before its actual onset (Greitens, 2020: 185). As a result, Taiwan in particular, may be considered an exceptional case where contact tracing has worked.

Following its experience with SARS in 2003, Taiwan was as well prepared as it could have been for the COVID-19 pandemic. The national pandemic response was approved by the Constitutional Court, which ensures that any policy adopted under an emergency health response will go through both judicial and legislative reviews and ratifications (Greitens, 2020: 184). This has been an important framework used to protect Taiwan's democratic system and its institutions. South Korea, on the other hand, has tried to work with its much more recent framework after the outbreak of MERS in 2015. Its judiciary developed a strong legal system to specifically address public health pandemics (Greitens, 2020: 184). Namely, the Infectious Disease Control and Prevention Act has been monumental in creating a transparent system with a big focus on accountability in the public health sector. Impressively so, the public health sector in South Korea has been responsive to national demands and concerns for data privacy in the early days of the pandemic. The National Human Rights Commission has made recommendations on which data should or should not be made public information (Greitens, 2020: 184).

Taiwan has also developed an impressive system through its system of collaborative governance. Collaborative decision making helps to foster mutual trust, access to resources, as well as a shared responsibility (Schwartz and Yen, 2016: 127). Collectively, Taiwan's acts, regulations and laws have been used to be able to prepare for and respond to the COVID-19 pandemic. Moreover, the digitisation of medical information has reportedly made the administrative costs of national health insurance extremely low (Da Silva, 2021: 443). The IC-chipped National Health Insurance card has also allowed doctors to have quick access to medical records and to monitor and detect COVID-19 cases in real-time (Da Silva, 2021: 443). The government in Taiwan uses a compulsory mobile phone location tracking service to ensure that one does not disobey quarantine

laws. To avoid exclusivity and to ensure that everyone has the same access to public health, the Taiwanese government has issued GPS-enabled phones to those in need (Kitchin, 2020: 363).

The Taiwanese government has been working with the tech industry for many years to help create online platforms and initiatives that will help citizens express their opinions and propose policy reforms (Tang, 2019). Taiwan created this political system by essentially crowdsourcing their democracy. Tang (2019), Taiwan's digital minister, also highlights how this very movement's inception was a result of a great national outrage surrounding a lack of openness and accountability in politics. In an attempt to change this, Taiwan's leadership connected with a group of people known as civic-minded hackers and coders with who they worked together to improve government transparency by creating open-source tools (Tang, 2019). In fact, the government first became aware of this group during the Sunflower occupation and protests, where they worked closely with protestors.

Before this, as early as 2014, government minister Jaclyn Tsai had been focused on digital technology and its significance in governance as a neutral platform for online communities to exchange policy ideas (Tang, 2019). This saw the creation of vTaiwan (virtual Taiwan), which is a collaboration of civic hackers and government to provide a platform upon which representatives of the public, private and social spheres to debate policy, particularly those pertaining to the digital economy (Tang, 2019). Thus far, vTaiwan has been extremely successful in tackling a multitude of issues. The open and direct lines of communication between the government and its citizens have been highly beneficial for both parties, particularly government officials who are constantly exposed to new ways of thinking as well as the most pressing public service demands and how to potentially address them (Tang, 2019).

Taiwan and South Korea have both adopted data first approaches, but Taiwan has ensured that all data collected will be deleted after the fourteen-day quarantine period is complete (Greitens, 2020: 183). More so, the government of Taiwan has ensured that it

will outdo the contact tracing system of monitoring when the pandemic has subsided and conduct audits where and when necessary (Greitens, 2020: 183). The South Korean government has also pledged to limit the retention of contact tracing data by allowing a select few government officials access to processing data. This is done over a processing platform that is strictly monitored to avoid any misuse or abuse of power (Greitens, 2020: 183). Similar to Taiwan, the government of South Korea has promised to discard such data collected after the pandemic has ended.

While South Korea ticks many boxes, it has not actually proven to be seamless in its approach. The government has not been entirely transparent through its contact tracing processes. A common fear of how data can be abused during the COVID-19 pandemic was brought to life when the government was found guilty of breaching citizen privacy and “outing” a big population of the country’s community of gay men (Fahey and Hino, 2020: 4). This kind of trolling is possible by tracking clusters of COVID-19 cases to locations where a big portion of the capital city’s gay bars are based.

COVID-19 contact tracing technologies are ultimately enabling a very sinister side to government surveillance. It has the potential to either strengthen already existing authoritarian regimes but also to erode the few democratic principles that seem to exist in today’s tightly monitored world. One might also consider both Taiwan and South Korea’s histories of authoritarian leadership which would have played a seismic role in creating a culture of acceptance of the law. In these moments, the power of governmentality and biopower are foreshadowed in implicitly directing citizen behaviour and choice. As a result, the people of Taiwan and South Korea have cooperated with governments in the emergency public health response to COVID-19, contributing to what has thus far appeared to have been a successful pandemic response.

3.8. Why preserve democracy?

The COVID-19 pandemic has exposed the abuse of power through surveillance tactics like data collection across many different regimes throughout the world. It is likely that such tendencies existed before the onslaught of the pandemic and the introduction of such technologies. However, the pandemic has allowed states emergency powers to hold an exceptionally tight grip over populations. Moreover, the COVID-19 pandemic is the first real global health emergency of its calibre to occur in the time of such advanced technologies, making it different to any other pandemic.

Take the (democratic) Republic of Singapore for an example. If an individual with the contact tracing app tests positive for the COVID-19 virus, the Ministry of Health may then upload data from the relevant app, enabling the government to trace to whom the smartphone belongs (Stevens and Haines, 2020: 524). This then allows the Ministry of health to trace those who may have come into contact with the virus and place the individual into quarantine. To develop the app, the Singaporean Ministry of Health, together with the police force, began the contact tracing process by collating data from personal interviews, using CCTV footage, following ATM transactions, using passenger data from airlines and transport companies, as well as cell-phone records (Stevens and Haines, 2020: 524). This is only possible through significant access to both personal and sensitive data.

Currently, around 80% of the Singaporean population has signed up to its contact tracing app, TraceTogether (Illmer, 2021). Government encouragement to download and cooperate with national usage of the app came from the angle that it was developed for citizen convenience and service, an act of goodwill to ease the blow of the pandemic at large. The government also made the promise that personal data would never be accessed for anything other than contact tracing in the case of testing positive for COVID-19 (Illmer, 2021). Yet, it has recently been discovered that the Singaporean police are utilising private data from contact tracing apps for more than just virus tracking (Illmer,

2021). Data from the TraceTogether app is now being used for criminal investigation, which the government has framed as a matter of public security.

In the meantime, Digital Rights Watch, an Australian privacy watchdog has expressed major concern, highlighting that the example of Singapore has to be one of the biggest fears of privacy advocates coming to life since the worldwide outbreak of COVID-19 (Illmer, 2021). It is a real time example of the erosion of public trust and the subsequent failure of an effective digital contact tracing attempt. It should also be considered that if state probing into personal life forms part of the greater pursuit for modernity, it becomes difficult to see the drive to collect personal data for contact tracing in isolation. One therefore comes to question and consider the intention of the state beyond the safety of its citizens.

Emergency powers and responses to the pandemic have raised fear of the rise in illiberal approaches to governance ahead of the pandemic. While surveillance measures have proliferated with the COVID-19 pandemic through different contact tracing measures used throughout the world, it is of critical importance that these measures remain proportional and are limited in their time frame. However, at the hands of the networked society and the global pursuit for modernity citizens all over are losing their sense of autonomy. Moreover, the narrative of upholding and protecting democratic principles holds little weight.

At this point, the work of Agathangelou (2008) will be used to slightly complicate the idea of, and the traditional understandings of democracy. Democracy as a political ideal has made tenuous promises of freedom and equality that should be protected by the notion of international human rights. Under democracies, therefore, one is led to believe that the system will ensure notions of safety and security. Thus, emergency measures like national lockdowns and contact tracing technologies are widely accepted in the name of safety and security. This process is also guided by the role of biopower and the powerful role of governmentality throughout society: to do the correct thing for the benefit of the community. Furthermore, this study aims to highlight how, in this democratic process that

promises ideals of safety and freedom, the creation of the “other” is necessary. After all, to be free or safe requires the creation of an unfree or an unsafe reality (Agathangelou, 2008: 120).

The process of creating the other helps to understand the different power dynamics within a society. In fact, the imperial project is reliant on the creation of bodies who do and don't belong (Agathangelou, 2008: 123). Certain marginalised bodies will always serve as the “raw materials” for the processes of democracy, upon whose daily deaths are depended on so that the idea of “spectacularized” murder is made possible (Agathangelou, 2008: 123). What is more, even within these marginalised communities, power dynamics exist whereby certain bodies are less excluded than others. Those who choose to partake in the system of capitalist democracy do so based on the belief that they will be granted equal rights that democracy promises. However, this is not the case. People or groups from marginalised and excluded communities may be accepted into the system based on their allegiance with the nation state with the goal of being incorporated into the “parameters of citizenship” (Agathangelou, 2008: 125). The contradiction is that this can only be done in exchange for violence because, after all, the democratic capitalist system will always necessitate the creation of a societal enemy that is used to create a sense of fear but also a sense of safety, freedom and protection.

Agathaneglou (2008: 125) summed this up using the example of how the white, upwardly mobile, good queer citizen has negotiated a space of belonging in democratic capitalist society. This dynamic should be understood as a “bargain brokered in exchange for closing his eyes to other kinds of violence committed daily on bodies of other queers, indigenous, black, and other people of color, the terrorists, and members of the working class” (Agathaneglou, 2008: 125). She further posits how democratic capitalist society is the result of a:

“Dual process by allowing white, middle-class lesbian, and gay sexualities to enter citizenship while simultaneously participating in the policing and criminalising of racially pathologised sexualities seen as threatening to the nation: the terrorist, the

inmate, the “welfare queen,” the illegal alien. Importantly, as this process of creating spectacularized or exceptional enemies unfolds, there is always a simultaneous production of nonspectacular others, those whose lives and deaths do not even register within this moral economy. These are the forms of predatory and pathological sexualisation that must be marked and liquidated for good (queer) citizens to stage their entrance into the body politic.” (Agathangelou, 2008: 127).

Agathangelou (2008) has been important in understanding the global responses to the COVID-19 pandemic; why people are willing to accept the different national emergency responses, and how citizens as well as countries at large are prepared to play blame games between one another. By looking at democracy from this perspective, the politics of the COVID-19 pandemic should be addressed with caution. Creating an enemy and building fear on both the local and the global scale is not unprecedented in history. It creates division and encourages a deeper dependence on security from the state. Ultimately, this will entrench existing unequal power dynamics throughout the world in the name of preserving the very overly celebrated system of democracy.

3.9. Making sense of the fears behind contact tracing applications

While breaching data privacy raises concern for the erosion of public trust, the abuse of personal data by national governments has given rise to far more sinister concerns. Further marginalisation of minority groups through the violation of their privacy, the exacerbation of discrimination and inequality are all real fears that the increase in digital health surveillance may bring to life. Along with the diminishing sense of public trust, citizens are losing their sense of personal autonomy.

In states that are using compulsory contact tracing apps, public and private service provision thus become contingent on downloading the relevant app (Sekalala, Dagon, Forman and Meier, 2020: 11). This creates a dangerous context in which those in positions of power may easily abuse their status, leading to a greater disconnect between people and the further entrenchment of inequalities. Similarly, when governments made

the distinction between essential and non-essential services and economic sectors that may consider operating during the height of the pandemic, they ultimately made a decision as to which bodies would be put at risk (Dias and Deluchey, 2020: 8).

The nature of essential service work is low paid and unskilled, meaning that the economically marginalised would likely be exposed to the virus and made more vulnerable. Not only is the pandemic worsening already existing inequalities by circumstance, but it is also having discriminatory effects on the social and economically marginalised groups in society. An established link between poor health and low socioeconomic living conditions can now be used to describe how the COVID-19 pandemic is impacting some people harder than others (Dias and Deluchey, 2020: 13). More so, contact tracing applications as technological solutions to mitigating the spread of the virus have been so focused on the issue of technological innovation that an informed public debate has been neglected. Consequently, the disproportional impacts of the virus on poor and economically marginalised communities have not been considered in the development and adoption of the contact tracing applications (Garrett, 2021: 11).

In the same breath, compulsory contact tracing applications are essentially creating a reality in which biology becomes a source of privilege (Kalpokas, 2020). What is more, those without access to smartphone technology or app access are immediately excluded from using them and in turn, excluded from the protection of the state. An example of this is in India, where the contact tracing app used has been made compulsory for all employees. The first major implication of this is the fact that employees immediately lose any kind of meaningful consent. Secondly, migrant workers face the potentiality of further marginalisation as they already often have fewer rights than other workers if they are, which is often the case on temporary, informal, or poorly constructed contracts (Sekalala, Dagon, Forman and Meier, 2020: 12).

Worse, the government along with its general population might not consider the marginalisation of the migrant population as a cause for concern. This is due to the all-

round precarity and disregard for migrants within society in general. It is likely that migrants will be further excluded from society as they take the blame for carrying and spreading the virus as a direct result of their precarious living circumstances. Context-dependent, the meaning of contact tracing technologies can be life-threatening for certain populations. This is proving to be the case in countries with an already authoritarian kind of government in power. A clear link between the use of contact tracing and social stigmatisation has therefore been established (French et al., 2020: 7).

Within disenfranchised communities alike, fears concerning the adoption of contact tracing technologies are real, widespread, and very valid. Generational inequality and discrimination have claimed many lives, and the COVID-19 pandemic may well make such inequities worse. In fact, before the onslaught of the COVID-19 pandemic, growing concern surrounding surveillance and the development of the global police state had grown out of the fears of the capabilities of new technologies and digitisation. Aspects of state surveillance through means of policing and repression have already crept into life with the development of technology and the rise of the so-called fourth industrial revolution (Robinson, 2020: 11). Surveillance technologies are enabling a global police state in which permanent warfare against marginalised communities exists, crushing insurgencies from below (Robinson, 2020: 11).

This safeguards the legitimacy of capitalist states in the wake of the recent economic collapse as the COVID-19 pandemic leaves a wake of inequality, global conflict, authoritarianism and social distress (Robinson, 2020: 11). Capitalist crises are typically synonymous with societal and class conflicts, which have been on the rise for many years now. Moreover, as states attempt to capitalise upon political power through the global health pandemic, opposition from below grows, and the world enters new and unimagined terrains of chaos (Robinson, 2020: 11). As chaos mounts, the world moves closer to a turning point whereby the capitalist socioeconomic system will need to be reimagined (Robinson, 2020: 12).

In these instances, the already disenfranchised and vulnerable groups in society are being disproportionately impacted by the pandemic and the rollout of responses and contact tracing technologies. In Qatar, for example, the contact tracing app used has been made compulsory, meaning that each citizen is then legally bound to own a compatible smartphone (Sekalala, Dagrón, Forman and Meier, 2020: 12). Should anyone refuse or not be able to download the app for any reason, they face a punishment of a \$55 000 USD fine and a potential three-year prison sentence. Statistically, these laws will affect at least 88% of Qatar's migrant population (Sekalala, Dagrón, Forman and Meier, 2020: 12).

Such arbitrarily enforced ultimatums are threatening the Qatari people's rights to privacy, bringing about more harm than good. Circumstances of this nature also contribute to the argument that contact tracing applications are simply inappropriate for low resourced contexts. They are exclusive by nature, failing to provide aid to those who really need it in poor and low resourced parts of the world. In these instances, the pandemic has the potential to strengthen already existing or inclined authoritarian regimes. Illiberal pandemic responses are strengthening unequal power dynamics through measures of public monitoring and control.

3.10. Contact tracing as technological solutionism: the system of surveillance capitalism

The commodification and utilisation of one's personal health data should raise serious concern for what this may mean and the potential of both public and private bodies who have access. There is often no guarantee that surveillance measures will only be used for the initial disease management purpose. Moreover, there is uncertainty around the period of time these surveillance measures may be used for. These concerns are not random but rather come from a history of how data can be used and has been capitalised on. The COVID-19 pandemic would not be the first time that "short-term emergency measures" have become "fixtures for life" (Harari, 2020). Based on emergencies in the past, it is known that the nature of emergencies is to "fast-forward historical processes" (Garrett, 2021: 14).

At the same time, the commodification of personal data like the Facebook and Cambridge Analytica scandal that have previously been proven to threaten one's privacy must also be discussed in the context of COVID-19 and the related contact tracing measures. Democratic principles have been seriously abused by the commodification of personal data under the nose of the world's supposed leading democracy, the United States. The possibility of this reality leads one to question what is possible in the context of emergency pandemic laws. The extension of surveillance capitalism through social media and contact tracing applications is problematic as there is no guarantee that the platforms are not using or releasing personal information for commercial gain (Mandeville et al., 2013: 49). Surveillance capitalism should be viewed in relation to the project of democracy and the overriding state agenda to monitor its population. More so, the creation of the other justifies state surveillance and is generally accepted as a measure used to secure its population.

The universal nature and wide adoption of contact tracing applications are also creating a reality where confidentiality may be easily breached by private companies despite public health policy on that issue. Whether a privacy policy in public health exists or not, the global pursuit for the eradication of the novel COVID-19 coronavirus is leading to breaches in privacy and confidentiality (Mandeville et al., 2013: 49). This, therefore, contributes to the evidence that the growing system of surveillance capitalism is obviating the already existing system while breaching an array of human rights (Mandeville et al., 2013: 49). The system of surveillance capitalism is sustained by capturing as much data as it possibly can and will therefore be entrenched by the introduction and use of contact tracing technologies.

Contact tracing as a public health response should include the issue of data justice and the ramifications of surveillance capitalism on social and economic justice (Dencik et al., 2016: 9). In the case of the COVID-19 pandemic, big tech corporates are positioning themselves in such a way that they may profit from the global health disaster. Therefore, this study aims to highlight the fundamental issue of surveillance capitalism and the fact that governments are working with these corporates to develop solutions which are

essentially reinforcing the global dominance and sovereignty of private industry (French et al., 2020: 5).

The rush of private-sector to innovate and promote contact tracing applications as vital tools for a pandemic response should not be seen in isolation from the great economic reward that is at stake (French et al., 2020: 1). The COVID-19 pandemic has magnified the global system of surveillance capitalism. At the same time, levels of desperation have pushed the world into a corner and lured states into adopting privately developed surveillance technologies. Therefore, the commodification of personal data and the use of contact tracing applications needs to be assessed using the perspective of the larger assemblage of tech dominance and sovereignty in the world system today. From this stance, the rush behind contact tracing applications is exposed. Rather than being developed for the sake of national safety and security, contact tracing applications would not work without the privately owned platforms and infrastructures that allow them to operate (French et al., 2020: 1).

Contact tracing applications are inextricably linked to a corporate world. Mobile phones that are required for the contact tracing processes are privately owned after all. In fact, French et al. (2020: 1) discuss how the privately owned operating systems of Apple and Android amass user data and contribute to profitable information holdings. Moreover, the corporate infrastructures and the commercial data miners connected to such companies have clearly outlined the connection between contact tracing applications and the system of surveillance capitalism. Through the implementation of contact tracing applications, individual user data sustains the raw materials needed to sustain the system of surveillance capitalism. In fact, against this backdrop, contact tracing applications may even be considered a product of surveillance capitalism that hooks and “lures users into their extractive operations in which our personal experiences are scraped and packaged” (Zuboff, 2019: 10).

These above-mentioned dangers and fears behind contact tracing applications have materialised in the form of oppression and discrimination of minority groups, reinforcing

existing oppressive social and economic relations (French et al., 2020: 7). For example, in Shanghai, there has been debate on creating a personal health index that will be used in an app that ranks the country's citizens on the basis of their health (Sekalala, Dagon, Forman and Meier, 2020: 12). Factors such as sleep, daily step count and alcohol and cigarette consumption will all be monitored. The publication of this data can impact some citizens' future access to public health care or potentially the denial or exclusion from some insurance companies (Sekalala, Dagon, Forman and Meier, 2020: 12).

This discrimination also comes in the form of differential pricing of insurance which ultimately impacts the human right to health. Ultimately, the commodification of one's personal data and the surveillance of it by the state is what feeds a system of surveillance capitalism. In parts of China, measures of control used to contain the coronavirus are being discussed as potentially permanent tools to track population health and behaviour through smartphones (Greitens, 2020: 173). Already existing and invasive measures of surveillance are being further entrenched into China's system of social control under the guise of public health and resuming life as it was before the pandemic.

3.11. The consensus on contact tracing applications in the COVID-19 pandemic

Social biases are therefore being reaffirmed through the data that contact tracing apps are obtaining. Surveillance has long been a tactic used by states to monitor populations, particularly minority ones. However, the fear is that digital contact tracing mechanisms now have the potential to intensify existing social and economic inequities (French et al., 2020: 7). This plays out as states use data from contact tracing applications to identify groups it wishes to target (French et al., 2020: 7). Similarly, contact tracing applications have been used to identify ethnic groups, neighbourhoods or communities where there have been COVID-19 outbreaks which has led to state violence and stigmatisation of these groups (French et al., 2020: 7).

An important distinction should therefore be made here and that is the relationship between the growing system of surveillance capitalism and the role of biopower as a

regulatory power. The importance of bodies and population control, which forms the basis of biopower, have significantly changed world politics. Control over human bodies through data collection and commodification are changing the shape of subjects of war and global capitalism. Power in the world system today no longer solely depends on geographical power as scores of personal data are proving to be an incredibly valuable source of currency.

After all, while the mainstream narrative that democracy is being eroded has been warranted, this study looks at the fundamentally flawed system at large. Discrimination in many forms, delayed elections, curfews, censorship of media and social media and the all-around increase in surveillance tactics have been adopted, accepted and normalised under emergency laws (Greitens, 2020: 178). The COVID-19 pandemic provides a justification for the introduction of such measures and the potential for the weakening of laws that monitor the media or, in some situations the civil-military relations (Greitens, 2020: 180). The emergency use of the military to strengthen policing around lockdowns has raised concerns surrounding the military invention in ordinary or daily life, raising fear around the potential for it to pave the way toward some kind of coup d'état (Greitens, 2020: 179).

However, this study argues that the very system of democracy is enabling these fundamentally unequal power dynamics in society. Through the creation of the other, the democratic system makes tenuous promises of safety, freedom and equality (Agathangelou, 2008: 122). As a result, citizens comply with the state's emergency pandemic responses based on the belief that it wants to save its people and protect it from the other. Therefore, those who choose not to cooperate with the state response are socially outcasted and shamed for being uncooperative and selfish, harming the state progress toward the running of the national economy which ultimately contributes to the larger system of global capitalism. Fundamental to these dynamics is Foucault's understandings of biopower and governmentality which are frameworks that have been used to understand how society have policed one another into complying with pandemic responses.

What is more, the incessant creep of state surveillance throughout the world and the already existing fears surrounding COVID-19 are being worsened as social anxiety escalates as a result of social media privacy breaches (Mandeville et al., 2013: 49). It has not been ensured that third-party companies will not benefit in a way that is unrelated to pure disease management, nor that governmental authority is in check and that no laws are be made arbitrarily. Contact tracing apps should be purely evidence-based as well as strictly temporary.

4. Conclusion

4.1. Why contact tracing applications fail

This study began by analysing contact tracing technologies in the context of emergency COVID-19 health responses in Asia, with a close eye on the Asian Tigers. The aim of this study has been to assess the efficacy of such technologies but primarily to determine their impact on civil liberties under democratic leadership. Emergency laws have, in many instances, violated core democratic principles like the freedoms of expression, association and movement. At first, this study was primarily concerned with the rise in surveillance and the potential for COVID-19 control measures to become fixtures for life. While it has been established that surveillance is an age-old tactic used by states to monitor the movements and behaviours of their population, this study observes that surveillance is notorious for its creeping potential. Worldwide concerns for public security resulted in a significant intensification of state surveillance with the 9/11 attacks on the United States.

Through rigorous analyses, it has been proven that contact tracing applications are too infantile to be introduced, rather proving to do more harm than good at this point. At the time of writing this study (June 2020), contact tracing applications were new on the scene, yet the race had begun to develop the best technology. However, what has been found is that too many regulatory and policy gaps are currently standing in the way of the existing and most widely used contact tracing technologies. Namely, open-source, blockchain and data networks. These problems relate to the cooperation with the General Data Protection Regulation (GDPR), which promises to inform users of their data retention and use, allowing consent and ensuring the deletion of data after the necessary use period. Nevertheless, the world rushes toward a future of invasive surveillance based on the tenuous promises that the government wants to ensure the safety and protection of its populace.

Therefore, this study fills a gap in the literature that punts Taiwan and South Korea's democratic pandemic response models and contact tracing applications as efforts that

the world can learn from. Democracy and human rights are no silver bullet to a safe or free life. The COVID-19 pandemic in particular has exposed the fragility of life under democracy and how spaces of belonging and protection are constantly being traded off between minority groups within the system. This study began looking at the ways democratic systems and the idea of human rights have been challenged through the COVID-19 pandemic. What it found is that the very system of democracy enables very unequal social relations.

This study has also taken a particular interest in the overall cooperation with COVID-19 protocol, specifically contact tracing applications, despite how they often blatantly disregard human freedoms and privacy. To make sense of this, Foucault's frameworks of governmentality and biopower were employed to understand the control over human bodies as the main subject of governance. State control measures are shaped in such a way that they can direct behaviour and encourage discipline between citizens who uphold COVID-19 protocol by policing one another, characteristic of liberal capitalist democracy, whereby citizens have historically been constrained to very "narrow confines of behaviour and subjectivity" (Agathangelou, 2008: 131). The result has been the creation of what Foucault referred to as "docile" and "compliant" bodies (Foucault, 1991). The role of biopower as a regulatory power, in turn, strengthens these surveillance technologies employed by the state. Therefore, the biopolitical architecture of the world is entrenched through the development of contact tracing applications that form part of an extension of state surveillance.

By working with the private industry to develop these applications, this study has highlighted Zuboff's (2019) argument that a system of surveillance capitalism is obviating the current global political system. This study has also framed the development of contact tracing applications as an extension of surveillance capitalism and in this light, more of a threat than a saving measure. Consequently, highlighting an important question of whether a marriage between civil liberties and public health could be a possible outcome from the COVID-19 pandemic. In the meantime, big tech corporations harvest, profile and commodify personal data, which is then shared and collaborated with national

governments to develop and strengthen surveillance technologies. Surveillance capitalism once again lures society into its operations through legitimate claims to hopefully provide a tool to ease the blow of the pandemic. In the same breath, contact tracing applications normalise and entrench the societal distinction between safe and unsafe bodies. Therefore, the biopolitics of the COVID-19 pandemic regulates private and public spaces, determining notions of belonging and citizenship.

4.2. Why democracy and human rights fail

On that note, Agathangelou's (2008) work has provided a critical framework on which this study bases its understanding of these very politics of belonging. Agathangelou (2008) is useful in helping to fill a gap in the available literature that often focuses on the importance of strong democratic institutions and their necessity to protect human freedoms under emergency pandemic laws. This study uses Agathangelou's (2008) understanding of democracy to make the argument that the politics of exclusion and a life of precarity will always exist for those who do not wish to cooperate in the larger system of global capitalist democracy. Thus, in the COVID-19 world, in order to believe that the state is protecting the safety and security of its citizens, it requires the creation of an unsafe reality. Therefore, the introduction of savings measures like contact tracing applications echoes the logic of the imperial project that relies on the notion that certain bodies do and don't belong in a society (Agathangelou, 2008: 123). Those who choose to cooperate with the state essentially form an allegiance with the global system based on the will to be accepted into the parameters of belonging. Those who choose not to cooperate will form part of the much necessitated "other" around whom notions of fear and unsafety are built.

It is important to understand how this dynamic is also reflected in the broader global system of politics. Wherein countries are demonised and red-listed for being central hotspots of the coronavirus. In fact, the recent discovery of the Omicron variant of the coronavirus in South Africa has been an important example of such politics. Despite the fact that South African scientists first identified the variant, there is still no evidence of where the strain may have originated (McKenzie, 2021). What is more, there is clear

evidence that the variant has been present in countries throughout the world since before the South African scientists identified that it was a new strain. In fact, it has been found that the virus strain has infected people in Europe who have not travelled to South Africa nor come into contact with someone who has (McKenzie, 2021). Despite the evidence, an imperial logic is applied, red-listing and punishing South Africa, causing a significant blow to the national economy. However, in doing so, powerful governments of the West are able to instil colonial-like fears surrounding the dangerous and unregulated Southern Africa. As a result, these governments are able to position themselves in such a way that they are protecting the safety of their citizens.

In the same way that the world turns a blind eye to these power dynamics, the data breaches and abuses by states to control minority populations occur. In addition, through these contact tracing purposes, the state is able to distinguish which bodies are worth putting at risk and on the line for the continuation of essential services. While the nature of essential work is low-skilled and low-paid, the socially and economically marginalised face further vulnerability in the face of the COVID-19 pandemic. What is more, those who do not have access to technologies required to download the contact tracing applications may be indiscriminately punished based on their circumstances. As a result, the COVID-19 pandemic is entrenching and exposing how biology becomes a source of privilege.

The introduction of contact tracing technologies is therefore having disproportionate effects on poor and marginalised communities. Where the app is made compulsory, those who do not have access are faced with arbitrarily enforced ultimatums. This was demonstrated using the example of Qatar and the heavy penalties and prison sentences associated with non-compliance to download the relevant contact tracing app. Similarly, in South Korea, the government have used data from contact tracing applications to troll and out gay populations. Nevertheless, South Korea has been celebrated by the media for its success in containing the spread of the coronavirus as one of Asia's leading democracies. The government outing of the South Korean gay populations has not been prioritised over the country's success in containing the spread of the virus.

Data privacy has been abused across both liberal and illiberal government contexts, pushing one to question the dangers behind the push for technological solutionism in the face of crises. Surveillance creep has had serious and lasting impacts in the past, leaving no reason why the coronavirus pandemic would be any different. In fact, the recent and rapid advances in digital technologies serve as even more reason to be concerned about the reproduction of the system of surveillance capitalism.

The COVID-19 pandemic has undoubtedly changed the landscape of world politics. Emergency health interventions and the use of contact tracing measures are seriously threatening the legitimacy of already weakening democracies throughout the world. Contact tracing applications employed under emergency health responses have, in many instances, proven to form part of a bigger system of surveillance. While such technologies may prove to be extremely helpful in specific contexts, they require strict monitoring and regulations. Political and economic power prevail as governments throughout the world rely on what Foucault refers to as governmentality, the social policing of one another between citizens. Contact tracing efforts have highlighted a host of human rights abuses and discrimination on already disenfranchised communities, entrenching existing power dynamics to the detriment of a widely celebrated system of liberal democracy.

As a world of mounting chaos is being pushed to a point where the world capitalist system ought to be reimagined. Existing power dynamics of the ruling groups of society, namely the state and, more recently, big tech, are being entrenched as the control of the masses has been concentrated into the hands of the elite minority. Digital contact tracing technologies used in the name of saving are enhancing control, and profit-making falls part of the very system of the fourth industrial revolution. The infrastructure of the fourth industrial revolution is arguably producing a new world order that is different to the system of global capitalism (Robinson, 2020: 11). Despite the many shortfalls behind the existing contact tracing applications, the race for mass data collection in the name of saving continues.

As the race continues, multiple questions merit further investigation. What does the future of world leadership look like, considering that the pandemic is exposing the spread of illiberal tendencies? Or, are the politics of exclusion that are exposed by the pandemic simply mirroring the existing power dynamics of the world system? Which other technologies that form part of pandemic response plans are threatening to worsen inequities in the same way as contact tracing apps and what policy is in place for these mechanisms? Can the mandating of the vaccine passport be seen in the same way as the contact tracing application? What standards and regulations are in place to stop the vaccine passport from also becoming an extension of surveillance?

References

Agathangelou, A. M. 2008. Intimate Investments: Homonormativity, Global Lockdown and the Seductions of Empire. *Radical History Review*. 100 (100): 120-143.

Bernal, P. 2016. Data gathering, surveillance and human rights: recasting the debate. 1 (2): 243-264.

Boersma, K., Van Brakel, R., Fonio, C., & Wagenaar, P. 2014. *Histories of State Surveillance in Europe and beyond*. London: Routledge.

Castells, M. 2009. *The Power of Identity, The Information Age: Economy, Society and Culture*. United States: John Wiley & Sons.

Castells, M. 2010. *The Rise of the Network Society*. United States: John Wiley & Sons.

Dias, B. L. C. V. & Deluchey, J. F. Y. 2020. The “Total Continuous War” and the COVID-19 Pandemic: Neoliberal Governmentality, Disposable Bodies and Protected Lives. *Law, Culture and the Humanities*. 00 (0): 1-18.

Dencik, L., Hintz, A. & Cable, J. 2019. Towards Data Justice: Bridging anti-surveillance and social justice activism. In *Data Politics: Worlds, Subjects, Rights*. London: Routledge. 167-186.

Fahey, R. A. & Hino, A. 2020. COVID-19, Digital Privacy, and The Social Limits on Data-Focused Public Health Responses. *International Journal of Information Management*. 1 (55): 1-5.

Foucault, M. 1978. *The History of Sexuality*. New York: Vintage Books.

Foucault, M. 1979. Discipline and Punish: The Birth of the Prison. New York: Vintage Books.

Foucault, M. 1991. The Foucault effect: Studies in governmentality. New York: University of Chicago Press.

Foucault, M. 2006. History of Madness. Abingdon: Routledge.

French, M., Guta, A., Gagnon, M., [Mykhalovskiy](#), E., Roberts, S. L., Goh, S., McClelland, A. & McKelvey, F. 2020. Corporate contact tracing as a pandemic response. Critical Public Health. 0 (0): 1-8.

Garrett, P. M. 2021. 'Surveillance Capitalism, COVID-19 and Social Work': A Note on Uncertain Future(s). The British Journal of Social Work. 1 (1): 1-18.

Greitens, S. C. 2020. Surveillance, Security, and Liberal Democracy in the Post-COVID World. International Organization. 1 (74): 169-190.

Guild, E. 2019. Data Rights: Claiming privacy rights through international institutions. In Data Politics: Worlds, Subjects, Rights. London: Routledge. 267-284.

Herrera, L. 2015. Citizenship under surveillance: Dealing with the digital age. International Journal of Middle East Studies. 47 (2): 354-356.

Idrees, S. M., Nowostawski, M. & Jameel, R. 2021. Blockchain-Based Digital Contact Tracing Apps for COVID-19 Pandemic Management: Issues, Challenges, Solutions, and Future Directions. JMIR Medical Informatics. 9 (2): 1-15.

Illmer, A. 2021. Singapore reveals Covid privacy data available to police. 5 September. Available: <https://www.bbc.com/news/world-asia-55541001> [2021, May 5].

Johnson, J. 2021. Worldwide digital population as of January 2021. 10 September. Available: <https://www.statista.com/statistics/617136/digital-population-worldwide/> [2020, September 23].

Kalpokas, I. 2020. The Biopolitics of Covid-19: The Pure Governmentality of Life [Presentation]. LCC International University. 24 August.

Kitchin, R. 2020. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tacking the spread of COVID-19. *Space and Polity*. 1-20.

Kosta, E. 2020. Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation and Governance*. 1 (1): 1-13.

Lyon, D. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, D. 2019. Surveillance Capitalism, Surveillance Culture and Data Politics. In *Data Politics: Worlds, Subjects, Rights*. London: Routledge. 64-77.

Madianou, M. 2020. A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic. *Social Media & Society*. 6 (3): 1-5.

Mandeville, K. L., Harris, M., Thomas, H. L., Chow, Y. & Seng, C. 2013. Using Social Networking Sites for Communicable Disease Control: Innovative Contact Tracing or Breach of Confidentiality? *Public Health Ethics*. 7 (1): 47-50.

Manokha, I. 2018. Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*. 16 (2): 219-237.

Mare, A. 2020. State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe. *International Journal of Communication*. 14 (1): 4244-4263.

Mohajan, H. 2018. Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*. 7 (1): 23-48.

Muller, B. J. 2011. Governmentality and Biopolitics. In *Oxford Research Encyclopedias*

Murray, D. & Fussey, P. 2019. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*. 52 (1): 31-60.

Olssen, M. 2007. Invoking Democracy: Foucault's Conception (With Insights from Hobbes). *Why Foucault? New Directions in Educational Research*. 1 (292): 205-226.

Osman, M., Fenton, N. E., McLachan, S., Lucas, P., Dube, K., Hitman, G. A., Kyrimi, E. & Neil, M. 2020. The thorny problems of Covid-19 Contact Tracing Apps: The need for a holistic approach. *Journal of Behavioral Economics for Policy*. 4 (1): 43-59.

Rabinow, P. & Rose, N. 2006. Biopower Today. *BioSocieties*. 1 (1): 195-217.

Robinson, W. I. 2020. Global Capitalism post-pandemic. *Race & Class*. 62 (2): 3-13.

Robinson, W. I. & Harris, J. 2000. Towards a Global Ruling Class? Globalization and Transnational Capitalist Class. *Science & Society*. 64 (1): 11-54.

Sawyer, S. W. 2015. Foucault and The State. *The Tocqueville Review*. 36 (1): 135-164.

Sekalala, S., Dagon, S. Forman, L. & Meier, B. M. 2020. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*. 22 (2): 7-21.

Schwartz, J. & Yen, M.Y. 2016. Toward a collaborative model of pandemic preparedness and response: Taiwan's changing approach to pandemics. *Journal of Microbiology, Immunology and Infection*. 50 (2): 125-132.

Stevens, H. & Haines, M. B. 2020. TraceTogether: Pandemic Response, Democracy, and Technology. [East Asian Science, Technology and Society: An International Journal](#). 14 (3): 523-532.

Tang, A. 2019. A Strong Democracy is a Digital Democracy. *The New York Times*. 15 October. Available: <https://www.nytimes.com/2019/10/15/opinion/taiwan-digital-democracy.html> [2020, March 21].

Tréguer, F. 2019. Seeing Like Big Tech: Security assemblages, technology, and the future of state bureaucracy. In *Data Politics: Worlds, Subjects, Rights*. London: Routledge. 145-164.

Marx Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.

Wilford, S. H., McBride, N., Brooks, L., Eke D. O., Akintoye, S., Owoseni, A., Leach, T., Flick, C., Fisk, M. & Stacey, M. 2021. The Digital Network of Networks: Regulatory Risk and Policy Challenges of Vaccine Passports. *European Journal of Risk Regulation*. 12 (2): 393-403.

World Health Organization. 2020. WHO Director-General's opening remarks at the media briefing on COVID-19. Available: <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> [2021, September 21].

Yen, M. Y., Chiu, A. W. H., Schwartz, J., King, C. C., Lin, Y. E., Chang, S. C., Armstrong, D. & Hsueh, P. R. 2014. From SARS in 2003 to H1N1 in 2009: lessons

learned from Taiwan in preparation for the next pandemic. *Journal of Hospital Infection*. 87 (4): 185-193.

Yeung, K. 2018. Algorithmic regulation: A critical interrogation. *Regulation & Governance*. 12 (4): 505-523.

Zuboff, S. 2019. Surveillance Capitalism and the Challenges of Collective Action. *New Labour Forum*. 28 (1): 10-29.