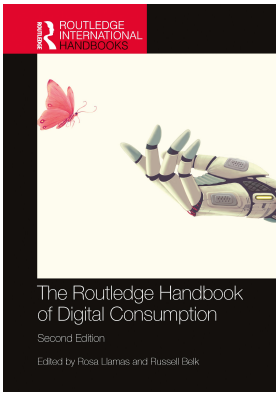

The Routledge Handbook of Digital Consumption

Rosa Llamas, Russell Belk

The Power of Digital Integration

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9781003317524-42
Guojun (Sawyer) He, Eric Ping Hung Li, Matt Husain
Published online on: 26 Sep 2022

35

THE POWER OF DIGITAL INTEGRATION

The Normalization of Tracking and Surveillance Technologies

Guojun (Sawyer) He, Eric Ping Hung Li and Matt Husain

Introduction

In the past decades, digital technologies such as big data analytics and artificial intelligence (AI) had transformed market operations and consumers' consumption practices substantially. These new digital technologies embed the marketplace novel services and communication channels, transaction platforms, business opportunities and models, thus providing consumers with new consumption experiences as well as new excitements and dreams forged on their use of these technologies. Since the end of 2019, the COVID-19 pandemic has increased online interactivity to an unprecedented extreme. As the pandemic surged, an increasing number of countries across the world have implemented nationwide confinement for months, resulting in the closure of brick-and-mortar-based goods and service providers such as movie theatres, shopping malls, and restaurants as well as the cancellation or postpone of large-scale public events such as popular concerts and sports tournaments. Consequently, as a recent survey commissioned by the United Nations Conference on Trade and Development (UNCTAD) indicates, consumers situated in the pandemic were turned to increasingly "embrace" digitalized methods in making their meaningful lives by relying on the internet for news and health-related information, daily shopping, and entertainment (McCourtie, 2020). All these facts illustrated the ever-growing importance of digital technologies in our consumer society.

While the new digital technologies offer great convenience and experience for both marketers and consumers, it generates new societal norms and expectations in tandem with new varieties of risks and concerns for consumers as well as a series of unknowns and uncertainties for user groups. Thus, in this chapter, we argue that the most recent advancement in digital technologies such as big data, AI, and any form of surveillance and tracking systems increasingly exacerbates fear and anxiety that echo what Orwell (1948/2014) infamously put it, "big brother is watching you". We structured this chapter by first underpinning the literature on the critiques of how governments and emerging or gigantic digital businesses often monitor and sell our digital footsteps as "raw data" to expand market base and increase profit margin. Next, we draw on Foucault's normalization and panopticonism, the two key constructs in his conceptualization of power (Foucault, 1978/1991), to explain the chapter's

DOI: 10.4324/9781003317524-42

theoretical grounding behind the practices of information monitoring and control under the overarching framework for regulation. The Foucauldian theoretical lens enables us to move to critically examine the case of China's most recent implementation of the Health QR Code (hereafter, HQRC) that was originally designed to contain the COVID-19 pandemic. Our analysis unfolds the significance of using and normalizing highly digitalized methods consisting of digital surveillance and tracking technologies to forge efficient governance at the expenses of consumer privacy. Following the case analysis, we discuss the intersection of governance and digital integration in a hope to demonstrate some worrying effects of establishing, exercising, and normalizing digitalized "meta-power" on civic freedom. This discussion affords us to briefly elucidate our thoughts on the managerial implications of our study, as well as map out future research avenues.

Digital Technologies and Digital Consumption

There is little doubt that we live in a digital society in which technologies can be considered a two-edged sword. On one hand, the new technologies offer tremendous convenience and efficiency. Amazon and other online marketplaces, for example, provide us access to millions of merchandises without leaving our homes. Moreover, Netflix converted our personal space into a theatre by connecting to thousands of TV dramas and movies at a relatively affordable monthly subscription fee. Airbnb and Uber changed the travel and transportation business models through specific sharing platforms. Also, an increasing power of social media such as Facebook, Instagram as new advertising and consumer engagement platforms is widely acknowledged. Unfortunately, at the same time, consumers are treated as "data" for these emerging (if not, gigantic) digital businesses. Our online activities, browsing history, purchasing track records as well as our networks and personal stories (e.g., images, videos, posts, and emotions) are now stored and often sold as "raw data" for data scientists to develop their next predictive analytic models or algorithms to take AI to the next level, all in order to increase corporate profit margin. David Lyon (1994) calls this ongoing cyber-surveillance in the new digital world "electronic eyes" (see also Lyon, 2006, 2007, 2011, 2018).

Over the last two decades, consumer researchers kept examining how market agents and consumers interact in the new digital platforms (e.g., Belk, 2014; Schau and Gilly, 2003). At the same time, researchers flagged concerns related to surveillance and breach of consumer privacy (Ashworth and Free, 2006; Ball, 2017; Lwin, Wirtz, and Williams, 2007; Milne and Culnan, 2004; Nguyen and Li, 2010). In this chapter, we define digital consumption as any internet or mobile phone-based consumption. Increasingly, surveillance, which is a new variant of digital consumption, has emerged as an activity that goes beyond to influence, manage, protect, or direct citizens that unilaterally claim private human experience as free raw material for translation into behavioural data. This constitutes the core security strategy for many nation-states and the core business model for the largest internet firms, for example, credit cards companies and advertisers (Lyon, 2007; Zuboff, 2019).

As all modern communication is digital, the frequency of surveillance increases in tandem. According to Sparrow (2014), "the relatively centralized nature of the core backbone of the internet makes it possible to monitor most of the world's traffic from a few key locations. Also, the rapidly falling cost of sensors to convert real-world inputs into digital signals has resulted in a proliferation of these sensors in our environment". The author also adds that information stored on servers in digital formats effectively lives forever, even very large datasets. The automated capture, storage, and analysis of such digital information exceed human capacity. For example, "the former East German secret police employed as many as 2 million

informants, but today it would require only a handful of off-the-shelf network monitoring devices, placed in key locations, to far surpass the Stasi's reach" (Koehler, 2000). The author concludes that automation enables state intelligence services and internet businesses to monitor user information with an idea that the data might be monetized in the future. We find the issues raised by these scholars reasonable and problematic in regards to the consumers' privacy aspect.

Government and private sector organizations often argue that the certain datasets they collect and maintain are anonymous because they do not include the real names of people. In reality, researchers including Narayanan and Shmatikov (2008) discovered that it is possible to de-anonymize nearly every such dataset. According to these scholars, "for certain types of information, like location and relationships, it often requires only a few points of data to unmask a person's identity by correlating with another dataset in which real names are known". This finding is another area of our scholarly concern.

We summarize that the digital revolution began with great promise but surveillance features began to exhibit alarming self-defying patterns. In particular, the lights, bells, and whistles of digital commerce make consumers blind and deaf to the ways high-tech corporations and states can undermine personal autonomy and erode democracy. Governments these days collect more data than they know how to effectively process, and by every passing day, unfortunately, we continue to live in an age where the management and processing of information has become an essential component of industry, agriculture, public health, military, and soon education – in other words, nearly every aspect of state management and private business. These systems all need information to function, and surveillance designed to feed these systems more information is getting better all the time. Therefore, the struggle for the future of digital communication – who can control the flow of bits and who can assign identity to those bits – is being actively fought on the terrains of politics, law, and technology. In the next section, we employ theoretical grounding to explain how the practice of information monitoring and control is normalized respectively by businesses and governments as a profit-enhancing apparatus and a regulatory framework.

Normalization in the Era of Digital Integration

Foucault's conceptualization of normalization refers to two types of power: disciplinary power and biopower (Taylor, 2009). His theorization of disciplinary power can be represented by his seminal work, *Discipline and Punish* (Foucault, 1975). Drawing on the intersection of sovereign power and the evolution of states' application of various punitive methods in western societies, Foucault exemplifies carefully designed a prison complex, in which state exercises disciplinary power to cultivate docile bodies to become obedient to state-advocated codes of conduct. The exercise of disciplinary power is accomplished by states' manoeuvre of space and light in a prison complex to forge a highly effective surveillance system known as panopticonism. It refers to a central tower that accommodates prison guards responsible for enforcing disciplines, and that is surrounded by a ring-shaped infrastructure with built in individual inmate cells. While the panopticon tower has windows, its central location prevents natural light from getting inside, which makes the inside rather dark. However, every individual cell surrounding the panopticon contains a small window facing outwards the ring-shaped complex, and a large cell gate facing towards the panopticon tower. Every prison cell is thus illuminated by natural light coming from the window and gate, generating the "effect of backlighting" (Foucault, 1975, p.200) that represents the key mechanism of panopticonism. This design clearly exposes every inmate's activities inside a prison cell to

guards placed in the panopticon, whilst an inmate can barely see the guards, who remain relatively invisible. The "effect of backlighting" contributes to training and producing docile inmates to become self-aware and self-disciplined as well as remain fearful of armed guards. It is because any wrongdoing spotted by the invisible surveillance could become a subject for inmate misconduct and then lead to punishment.

Taking it beyond the prison context, Foucault (1975) argues that the surveillance-centred panopticonism was widely seen and operated in other institutions such as schools, hospitals, and army bases, in which a small number of people (e.g., teachers, doctors, and military officers) are empowered by states to cast a gaze on a large number of individuals (e.g., students, patients, and soldiers) and to evaluate these individuals' conduct according to rules and regulations set by states. These institutions are considered as disciplinary apparatuses functioning to identify, punish, and correct deviants, thus making state-advocated agendas social norms. In the context of disciplinary power, normalization refers to the panopticonism-fuelled and disciplinary apparatus-operated process of establishing, enforcing, and sustaining agendas set by states.

Since 1976, Foucault has worked on theorizing biopower, a concept that he coined in the first volume of *History of Sexuality* (Foucault, 1976 [1978]) and defined as "an explosion of numerous and diverse techniques for achieving the subjugation of bodies and the control of populations" (p.140). While still focusing on the production of docile bodies, Foucault's biopower construct described states' control over a population by not only relying on punitive techniques, but also by making efforts in forging "a form of activity aiming to shape, guide or affect the conduct of some person or persons" (Gordon 1991, p.2). Accordingly, unlike in the context of sovereign power, in the biopower setting, state-advocated social disciplines were diffused to societies aiming at convincing a population to view these disciplines as social norms. As Foucault (2003) explained, "the discourse of disciplines…is about a rule: not a juridical rule derived from sovereignty, but a discourse about a natural rule, or in other words a norm. Disciplines will define not a code of law but a code of normalization".

Foucault's development of biopower has twofold implications on the concept of normalization. First, normalization is a process of impelling state-advocated agendas to a population and convincing the population to follow, so that such agendas are transformed into social norms. Second, unlike the exercise of disciplinary power, which centres on punitive techniques largely implemented by state-controlled institutions, states' exercise of biopower includes the mobilization of non-institutional entities, which serve to diffuse social disciplines to a society as guidance for a population to foster lives, that is, "overall characteristics specific to life, like birth, death, production, illness, and so on" (Foucault, 2003, p.243). Accordingly, the concept of apparatus is broadened to include biopower apparatuses referring to any individuals, institutions, symbolic and material sources, as long as they contribute to the normalization process of transforming state-advocated agendas into a publicly recognized social norm. As Agamben's (2009, p.14) explains, "apparatus is literally anything that has the capacity to capture, orient, determine, intercept, model, control, or secure the gestures, behaviours, opinions, or discourses of living beings. Not only, therefore, prisons, madhouses, the panopticon, schools, confession, factories, disciplines, juridical measures…but also the pen, writing, literature, philosophy, agriculture, cigarettes, navigation, computers, cellular telephones…".

The Foucauldian conceptualization of normalization as a process and the roles of biopower apparatuses in the process has crucial implications in the contemporary consumer society. Nowadays, in the exchange of better individualized consumption experience, consumers are often convinced by companies to partially give up their privacy and allow companies to

use digitized technologies to trace and analyse their activities and interactivities in real time (Bardhi and Eckhardt, 2017). As consumers are increasingly relying on using digital devices in their daily lives, they are cultivated by companies to become more lenient with digital surveillance. This opens up the opportunities for public agents to join with commercial institutions in order to strategically normalize the use of digital instruments to cast a gaze on consumers from all possible perspectives of their lives. In the following section, we take a historical perspective to illuminate the evolution and normalization of a digital surveillance consumer society in China.

Illustrative Case Analysis: The Socio-Historical Development of Digital Surveillance and Tracking Technologies

In the development of digital surveillance and tracking technologies, China is among the most advanced countries in the world. Since the early 2000s, starting from Shenzhen, the Chinese central government has launched a massive surveillance system aiming at installing facial-recognition-enabled surveillance cameras nationwide (Bradsher, 2007). To make the public accept millions of surveillance cameras installed along streets, the state stressed the effectiveness of these cameras in helping police accurately identify suspects, regulate unusual social conduct, fight crime, and thus provide the Chinese population with a secure and safe living environment (Bradsher, 2007). In the same period, a new generation of chipped residency cards were introduced to Shenzhen residents first and then distributed to all Chinese people. Soon after, nearly every Chinese citizen has all of his/her personal data (name, address, work history, educational background, religion, ethnicity, and medical records) stored on the chipped card. Since all personal data was readily accessible at any time by the police or national security forces, the state's promotion of the chipped residency cards essentially digitalized the Chinese population, converting Chinese citizens into traceable targets that are subject to the monitor and intervention casted by disciplinary apparatuses. For this reason, the public expressed their concerns about the potential impacts of the schemes of the surveillance camera and the chipped residency cards on compromising Chinese citizens' privacy (Bradsher, 2007).

Despite the controversy, in 2014, the state sought to construct a "creditable society (诚信社会)" and launched the Social Credit System (hereafter, the SCS), a more advanced big-data-driven surveillance system that has been studied by Li et al. (*2021*). According to the authors, the SCS was built by both disciplinary and biopower apparatuses, such as central and local authorities, judiciary courts, the People's Bank of China, as well as Alipay and WeChat Pay, the two predominant moneyless payment providers belonging to Chinese e-commerce giants Alibaba and Tencent, respectively. The operation of SCS relied on gleaning a massive amount of data from consumers' financial and consumption activities by tracking the conduct of moneyless payment users' online and offline purchase, and their personal and commercial loan and payback records. Once collected, the data was subject to big data analysis in order to help form and sustain a reward-penalty system that is built upon to evaluate the "trustworthiness" of individual firms and citizens and assign them "social credit scores". Recipients of high scores are "red-listed" and rewarded to, for instance, have easier access to public and commercial services (e.g., schooling, health care, and consumer goods rental). People with low scores are "black-listed" and sanctioned by juridical courts, which restrict these individuals' consumption of pricey items and services (e.g., luxury hotels and first- and second-class public transport tickets) and deprive their community welfare eligibility (Creemers, 2018). As Li et al. (2021) concluded, the big-data-fuelled reward-punish

system, along with its unpublished scoring mechanism, forms a digital panopticon that generates the backlighting effects to help the state identify, punish, and correct deviants through quietly observing people's consumption-related activities, thus aligning Chinese social actors' dealings with consumption to state-advocated ways. As an ongoing surveillance scheme, the SCS continuously inspires the state and local authorities to extend the use of big data to shape people's conduct beyond consumption. For instance, in 2016, to enforce the state's advocate of waste sorting, the Beijing municipal government launched a QR code app requiring residents to use their phones to scan when disposing unwanted goods. Residents identified with well self-disciplined waste sorting individuals were rewarded with coupons for acquiring rice, soap, or cash in participating local grocery stores (Lai, 2016).

In late 2019, the COVID-19 pandemic erupted. In this pandemic, the state extended its use of big data to the public health arena to track and analyse citizens' health conditions. Two months into the pandemic, in the beginning of February, 2020, the state introduced the Chinese Health QR Code (hereafter, HQRC) to gain real-time information of the spread of the coronavirus. The HQRC came with two versions that were created in Shenzhen in a matter of a few days by state-mobilized software engineers from both disciplinary and biopower apparatuses: the Alipay version (hereafter the AHQRC) developed by police officers and engineers from Alibaba as a mini app embedded in Alipay and the WeChat version (hereafter the WHQRC) made as a mini app embedded in WeChat by Tencent (Tencent News, 2021; Tencent Technology News, 2020). Since both Alipay and WeChat had billions of active Chinese users nationwide, the AHQRC and WHQRC were quickly diffused from Shenzhen users to other users from hundreds of Chinese cities and were used by billions of times by March 2020 (Tencent News, 2021; Tencent Technology News, 2020). On the 1st May 2020, to paving the way for promoting the HQRC on a national scale, the State Administration for Market Regulation issued the "National Standard of Personal Health Information Code" to regulate and standardize the HQRC's data collection and analysis and to stimulate mutual recognition of the AHQRC-WHQRC among different cities and provinces (Guangming Daily, 2020).

The HQRC was designed to glean individual citizens' comprehensive personal data. To use the HQRC on mobile phones, users needed to register first by going through a "real-name verification" process asking for their real names and the corresponding identification numbers (Tencent Net News, 2020). Users were then directed to submit their "basic information" consisting of contact numbers, detailed residential location, and their "health conditions" (e.g., whether having contact with people contracted the virus). Finally, users were required to declare the truthfulness of the data they provided to have auto-generated Unique Individual Health QR Codes displayed on phone screens (hereafter, the UIHQR). The UIHQR came with three colours that are meant to change from one to another. Depending on the initial information recorded, the UIHQR may display on the phone in the colour of either green, yellow, or red. The green UIHQR permits users to move freely, the yellow one requires users to have a quarantine up to seven continuous days, and the red one asks users to self-quarantine for 14 continuous days.

The mechanism that triggers colour change is driven by a big data monitor and analysis of users' daily activities. Specifically, when users launch the HQRC in either Alipay or WeChat, they grant it the permission to gather up-to-date private information through invoking a number of mobile phone services and functions, such as the precise and real-time location (GPS) service, and the access to phone camera, microphone, and phone ID, number, contacts, and storage. Upon the launch, the HQRC simultaneously visits users' big database in the servers of Alibaba and Tencent, which have tracked and recorded over 74% of the

entire Chinese population's daily online and offline purchase (People's Daily, 2021) since 2014 for the abovementioned ongoing SCS scheme. Taking all data together, the HQRC immediately starts analysing and tracking, at the very least, places where people visit or been lately, and their recent medical records in hospitals (Tencent Cloud Community, 2020). In a few seconds, the HQRC produces precise information about users' daily consumption records and recent travelling trajectories that are decisive to trigger the colour change of the UIHQR. For instance, if a person is detected by the HQRC to have the record of buying public transport tickets to high COVID-19 risk areas, and of goods purchase or hotel check-in there, his/her UIHQR colour would be changed to yellow or red (Tencent Cloud Community, 2020). The colour change information is then transmitted to local authorities responsible for dispatching officials and volunteers to visit the person to enforce the corresponding self-quarantine regulation (Peng, 2020). In this way, the HQRC serves as a disciplinary device surveilling and regulating people's conduct in the pandemic.

The full disciplinary power of the HQRC is unleashed by the state's efforts in mobilizing both disciplinary and biopower apparatus to diffuse and mandate the use of HQRC in people's daily life. Specifically, HQRCs are printed off and displayed on billboards in every entrance of public spaces, such as residential areas, restaurants, metro and train stations, airports, hospitals, schools, local convenience stores, and shopping malls. Acting as disciplinary apparatuses, policemen, security guards, or community volunteers are recruited and dispatched by the local authorities to guard these entrances. The guards serve to ensure that every individual who wants to enter must use the HQRC to scan the HQRCs to immediately permit the big data analysis generating a UIHQR code. Depending on the colour of the UIHQR code, guards then either permit the person to enter or ask the person to leave and carry out self-quarantine. Given that entering public spaces is inevitable in daily lives, installing and using the HQRC becomes inescapable for the population, leading the entire Chinese population to submit themselves to the tracking, scrutinization, and analysis of the HQRC. Simultaneously, acting as the most influential biopower apparatuses, mass media outlets also strive to produce the knowledge about the usefulness and effectiveness of using the HQRC in fighting the pandemic. For instance, the *People's Daily*, the state-owned dominant official mass media (Zhao and Belk, 2008), lists a twofold benefit of using the HQRC (Peng, 2020). First is because the HQRC invokes big data and operated in prevailing mobile phone applications. Second, the HQRC effectively enabled the state to better identify and quarantine "contaminated" individuals to contain the pandemic, because individual health reports generated by the big data HQRC were deemed highly accurate, reliable, and up-to-date. Similarly, the *Chinese Communist Party News* also stressed that the nationwide HQRC mandate helped minimize the otherwise damaging impacts of the pandemic on the national economy, for it precisely identified uncontaminated individuals based on real-time data to permit them to return to work (Wang, 2020).

Similar to the ongoing big-data-driven SCS schemes, the HQRC mandate sparked the controversy over the state's violation of people's privacy (Zhao, 2020). Although the state and the companies involved in the research and development of the HQRC revealed principles of their handlings of users' personal information, they kept nuanced details about data collection, analysis, storage, and destruction remain unspecified and opaque to the public (Du, 2020). The HQRC thus situated users in a vulnerable situation, wherein they are fully aware of the digitalized comprehensive surveillance, but have neither the knowledge about nor the control over the extent to which the digitalized surveillance would only be used to address the public health crisis. To some extent, such concern is triggered by the state's intention to extend the use of HQRC beyond the original scope of containing the virus. In Du's (2020)

alarming article, the state's intention refers to its efforts in normalizing (常态化, *chang tai hua*) the HQRC. According to Du (2020), the normalization effort was first made by Hangzhou Municipal Health Commission. On the 22nd May, 2020, the Commission held a special conference and tabled the normalization plan of the HQRC. The plan sought to authorize HQRC to further analyse all possible big data in order to allow the government to guide the population to live in healthy lifestyles in the post-pandemic era. Accordingly, the Commission allowed the HQRC to extensively collect data from all perspectives of users' lives (e.g., the records of medical visits and health checks and of consumption of tobacco and alcohol) in order to monitor and shape individual citizens' lifestyles in the name of health in the post-pandemic context. The further analysis aimed to generate "Health Evaluation Reports" that are coded no longer in three colours used in the UIHQR, but in colour gradient from green to yellow to red. These colour-coded reports were meant to enable the local authority and public health department to first evaluate and grade people's health collectively in the units of residential building, community, and companies. Next, individuals who have their reports in colours signalling "unhealthy lifestyles" (i.e., colours close to yellow and red) would then be alerted by the HQRC to alter certain consumption behaviours and lifestyles deemed unhealthy. In this way, the normalization of the HQRC affords the state to not only fight the virus, but also guide people to foster lives in designated "healthy" ways in the post-pandemic era.

In June 2020, as Lv (2020) documented, a state-advocated "Smart City" agenda was defined and stressed by the Chinese sitting President Xi Jinping as a scheme aiming to "use cutting edge technologies such as big data, cloud computing, blockchain, and AI to improve the management of cities, models of productions, and innovation. Making cities smarter, and more intelligent is the inevitable pathway to take in order to improve the modernization of the system and capability of city management". Xi's vision on the "Smart City" permitted the extensive use of big data analysis for governance purposes, thus paving the way for normalizing the HQRC beyond Hangzhou. Echoing to Xi's remark, in August 2020, the *People's Daily* began impelling the normalization of the HQRC and framing such normalization as a result of people's demand that is aligned to the "Smart City" agenda:

> The future [use] of the HQRC can be seen from a survey conducted by the People's Think Tank. More than 90% respondents hope that the HQRC can play even more important roles in the post-pandemic era, especially in the areas of public hygiene and health, city management, public transports and travelling, and popular culture and entertainment.
>
> *(Peng, 2020)*

From this point onwards, an increasing number of Chinese cities continuously endeavoured to normalize HQRC as a useful digital tracking device that "enables local governments to accurately gain data about all visitors and local residents' travel histories, and allows companies to precisely know the real-time data of employees' health conditions and movements" (Yu, 2021).

Discussion: Intersectionality of Governance and Digital Integration

Based on the illustrative case shared above, apparently China's response to the events the pandemic has set in motion a security agenda that aims to protect the country's public health and infrastructures. At the same time, it also appears to negatively affect civic freedom by

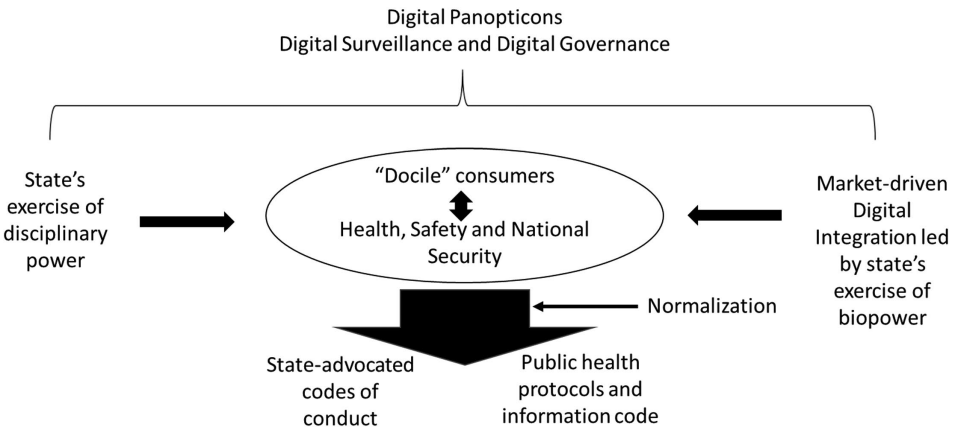

Figure 35.1 Conceptual framework
Source: Own elaboration.

heightening policing of individuals (Du, 2020; Zhao, 2020). The two emerging characteristics of this security agenda, in particular, the health app in light of modern power relations include: (a) the articulation of the health and safety of the Chinese population as a primary objective and (b) the emphasis on surveillance. These characteristics inform an approach that rationalizes China as a sovereign state oriented to ends-means strategies. In addition, it radiates a centralized message that the people of the country require subjection to regulatory mechanisms so that they can be protected from an overarching variety of possible, probable, and imagined threats that are placed under an ambiguous rubric of health, safety, and national security (Figure 35.1).

These interpretations are premised upon Foucault's (1997) postulation that modern society is marked by biopower, which is a mechanism of power mainly encompassing the management of biological life. In addition, as Bell (2006, 149) puts it, "as a power focused on life, biopolitics has meant that the problem of how best to govern has not only been posed in terms of effecting ultimate dominion over a sovereign territory, but increasingly as an issue of yielding productive services from the citizenry". As Gordon (1991) elaborates echoing Foucault, "'reason of state' is no longer confined to the will of the prince, but is 'government in accordance with the state's strength', which includes the 'ends-means' instrumental rationality associated with state survival in a competitive international system conjoined with the observance of what is governed and how government might improve or enhance the qualities of a population" (Gordon, 1991, pp.9–10). That may infer China is not the only state in the list that exercises a robust citizen monitoring and/or control apparatus.

Overall, scholars including Bell (2006), Dillon (1995, 2004), Esposito (2008), and Rose (1999, 2001) critique that the normalization of the biopolitical character of the state greatly reduces the traditionally accepted distinctions and boundaries between the state: (a) as a military and legitimated actor and (b) as a service-providing, regulatory agency for the management of the population. The confluence re-produces "the state as a pre-eminent, direct authority, but ushers in a set of decentralized and indirect mechanisms of rule that are principally activated through population monitoring" (Bell 2006, p.149). She problematizes a gap within the security agenda between securing the health and safety of the national population from threats and the indifference and breach of human rights and

freedom that may be at stake in such actions. Once enacted, a government can subjugate bodies, and Rose (1999) explains that such technologies of security are "'designed in' to the flows of everyday existence" (Rose 1999, p.234). This further illuminates the establishment of HQRC app in the case of China and its enactment of controlling citizens through a meta-database, which exemplifies governance through voluntary subjectification of citizens. In this case, moreover, technologies of security offer a persona that freedom is not being constrained, rather it is encouraged by mechanism of security and a source of empowerment (Dillon 1995, p.324). On the surface, this non-punitive method successfully facilitates the formation of social norms that tell people how to become good citizens (Rose 2001, p.6). The outcome also fulfils a political authority's wide-ranging pluralist aspirations that shape the perception and activities of its citizens in exercising their own freedom (Bell 2006; Dillon 2004).

Rose (2001) argues that this is how a political authority, primarily guided by biological, vital concerns, can optimize and regulate life by identifying and neutralizing random elements or "problems" within a population to address elusive "threats", often expressed through discourses of "risk". As a result, such an authority designs a "nationally organized and politically directed programme to improve the quality of the national stock and eliminate taints or weaknesses that might threaten it" (Rose 2001, pp.2–5). He explains that such a system is designed to sell the enmeshed narrative of the care and protection of life to the constituted threats. As he puts it, "liberal societies have come to posit the health of individuals in terms of the fitness of national populations (as seen in neo-hygienist and eugenic programmes), and states are obliged to guard the population from threats and to enhance fitness through competitive interstate projects. Risk as a distinctive means by which to spread security can, therefore, lead to the design of policies to detect unsecured, and therefore 'dangerous', lives, while simultaneously situating such actions in the realm of 'life' and beyond political inquiry or debate" (Bell 2006, p.152; Rose 2001, p.5).

Esposito (2008) echoes similar insights provided by Rose and Foucault, but steps up farther and defines biopolitics as a regime, in which "the protection of the biological wellness of the subject (even and especially if collective) hinges on the sanctioned extermination of the Other: the Other posited as a source of pandemics, hence annihilation, not of a particular body but of 'human being,' of the species. Biopolitics plants the destruction of humankind into the global or national political scene to justify, without grounds, the most brutal and/or absurd countermeasures" (Esposito 2008, p.9). He draws examples from the post-9/11 bombing of Afghanistan, in which war was waged in the name of the defence of humanity rather than of a state, nation, ethnicity, or religious group; the Russian police force's use of lethal gas to overcome Chechen kidnappers in a Moscow theatre, an episode that resulted in 128 fatalities (of hostages and insurgents); and the 2003 drawing of blood (for pay) from Chinese peasants as a few examples of the horror of biopolitics (2008, p.239). Esposito critiques biopolitics as a contemporary manifestation of this politics, in which the endangered subject obliterates alleged sources of danger through the very signature of modernity: technology. Finally, he urges people to seek alternatives by following the traces of biopolitics that leads to so called normalization (2008, p.194). This begs a query and discussion on the premise of tracing meta-data and seeks for alternatives.

Our illustrative case also suggested the new "proactive" governance approach that new digital technologies offered to governments and local authorities. AI-driven predictive analytics now become an important tool for preventing harmful behaviours. On the one hand, such surveillance technologies become a public good to maintain the societal orders and the

harmony of the society. On the other hand, the new technologies further limited consumers' freedom and rights – from freedom to travel to freedom to speech, and from freedom to consume and from the rights to be informed. Furthering the discussion of Mellet and Beauvisage's (2020) discussion on the "cookification" of the digital economy, the current chapter presents new concerns on the new surveillance technologies' capability to inter-connect consumers' digital and physical activities.

Conclusion

In this chapter, we focus on analysing digital surveillance and tracking technologies as a form of digital regulatory systems that monitor personal and institutional activities amid regular consumption and business. We also examined an intersection of governance approach and digital technologies to unpack the relationship between installing comprehensive digital tracking systems in a society and employing meta-data to monitor and/or control citizens. The additional motivations behind enacting such a digital apparatus include enhancing corporate profit and tightening a regulatory framework at the expense of breaching consumer privacy and human rights. We critique these worrying consequences of normalizing the invasive tracking technologies. It is because the formation of states' "meta-power" stems from digitizing all possible social and business activities of people into a meta-database, which continues to cast a gaze upon and regulate every possible aspect of people's lives, from birth to death.

Managerial Implications

In this study, we illustrated how meta-data can contribute to a state or government's public health protocol. In particular, the illustrative case study on China's HQRC highlighted the dilemma between consumer privacy and national safety and security. Private corporate and public policymakers, in this sense, need to identify a mutually accepted mechanism to ensure consumers' rights and national safety and security. Our study also sheds light to consumer advocates where responsible data integration policy and strategies are needed to ensure the future use of consumer data in the age of digital economy.

Managerial Implications and Future Research Directions

This study presents how the latest digital technologies allow key stakeholders such as private corporate and governments integrated consumer-citizens' data to create a meta-governance mechanism. Such data integration not only illustrates the capability of new technologies but also raises a number of concerns related to consumer privacy and corporate responsibility. As exemplified in the SCS case in China, a digital panopticon via HQRC, which is built by both disciplinary and biopower apparatuses, allows the state to scrutinize all Chinese social actors' consumption-related activities. Admittedly, the state initially developed several digital surveillance technologies in order to address urgent needs deriving from issues concerning public security, safety, and health. However, we sought to call for future research on the state's subsequent efforts in making digital surveillance a social norm. Accordingly, the established and promoted intersection of the evolving (digital) technology, consumer privacy, and the state's intensified digital surveillance calls for the needs of more scholarly discussion on governance merits in the era of digitalization.

Further Reading

Crampton, J. W., & Elden, S. (Eds.). (2016). *Space, knowledge and power: Foucault and geography*. London and New York: Routledge.

Fuchs, C. (2020). *Communication and capitalism: A critical theory*. London: University of Westminster Press.

Larner, W., & Walters, W. (Eds.). (2004). *Global governmentality: governing international spaces* (Vol. 28). London and New York: Routledge.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London: Routledge.

Schuilenburg, M., & Peeters, R. (Eds.). (2021). *The algorithmic society: Technology, power, and knowledge*. London: Routledge.

References

Agamben, G. (2009). What is an apparatus? and other essays. In What is an apparatus? and other essays. Stanford, CA: Stanford University Press.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. Journal of Business Ethics, 67(2), 107–123.

Ball, K. (2017). All consuming surveillance: Surveillance as marketplace icon. Consumption, Markets and Culture, 20(2), 95–100.

Bardhi, F., & Eckhardt, G. M. (2017). Liquid consumption. Journal of Consumer Research, 44(3), 582–597.

Belk, R. W. (2014). Digital consumption and the extended self. Journal of Marketing Management, 30(11–12), 1101–1118.

Bell, C. (2006). "Surveillance strategies and populations at risk: Biopolitical governance in Canada's National Security Policy." Security Dialogue, 37(2), 147–165.Bradsher, K. (2007). China enacting a high-tech. Plan to Track People. https://www.nytimes.com/2007/08/12/business/worldbusiness/12security.html

Creemers, R. (2018). China's social credit system: an evolving practice of control. Available at SSRN 3175792.

Dillon, M. (1995). Sovereignty and governmentality: From the problematics of the "New World Order" to the ethical problematic of world order. Alternatives, 20, 323–368.

Dillon, M. (2004). The security of governance. In Global governmentality: Governing international spaces. William Walters & Wendy Larner (Eds.), pp. 88–106. London: Routledge.

Du, H. (2020). The alleged violation of citizens' privacy: the colour gradient version of Health QR Code promoted in Hangzhou. Souhu News. May 25. Available at: https://www.sohu.com/a/397531243_665455 (Retrieved on December 19, 2020).

Esposito, R. (2008). Bíos: Biopolitics and philosophy. Trans. Timothy Campbell. Minneapolis, MN: University of Minnesota Press.

Foucault, M. (1978/1991). Governmentality. In The Foucault effect: Studies in governmentality, Graham Burchell, Colin Gordon, and Petter Miller (Eds.), pp. 87–104. Chicago, IL: University of Chicago Press.

Foucault, M. (1979 [1975]). Discipline and Punish: The Birth of the Prison, trans. A. Sheridan. New York: Vintage

Foucault, M. (1997). Society must be defended: Lectures at the Collège de France 1975–1976, trans. David Macey. New York: Picador.

Foucault, M. (2003). Society must be defended": Lectures at the Collège de France 1975–1976, trans. David Macey, p. 242. New York: Picador.

Gordon, C. (1991). Governmental rationality: An introduction. In The Foucault effect: Studies in governmentality, Burchell, Graham, Colin Gordon, & Peter Miller, (Eds.), pp. 1–51. Chicago, IL: University of Chicago Press.

Guangming Daily (2020). The national standard of personal Health QR Code published. Guangming Daily. May 02. Available at: https://epaper.gmw.cn/gmrb/html/2020-05/02/nw.D110000gmrb_20200502_5-03.htm (Retrieved on December 25, 2020).

Koehler, J. (2000). Stasi: The untold story of the East German secret police. Boulder, CO: Westview Press.

Lai, X. (2016). Trash cans are smarter, is it difficult to sort them? People's Daily Online. http://env.people.com.cn/n1/2016/0729/c1010-28593845.html.

Li, E. P. H., He, G. S., Lam, M. M. L., & Liu, W. S. (2021). Utopia and Dystopia: Consumer Privacy and China's Social Credit System. In Consumer Culture Theory in Asia (pp. 159–178). New York: Routledge.

Lv, J. (2020). Taking the construction of smart city to a whole new level. People's Daily. June 16. Available at: http://paper.people.com.cn/rmrb/html/2020-06/16/nw.D110000renmrb_20200616_2-09.htm (Retrieved on December 25, 2020).

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science, 35(4), 572–585.

Lyon, D. (1994). The electronic eye: The rise of surveillance society. Minneapolis, MN: University of Minnesota Press.

Lyon, D. (2006). Theorizing surveillance: The panopticon and beyond. Cullompton/Portland, OR: Willan Pub.

Lyon, D. (2007). Surveillance studies: An overview. Cambridge/Malden, MA: Polity.

Lyon, D. (2011). Why where you are matters: Mundane mobilities, transparent technologies, and digital discrimination. In ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks, pp. 222–236. IGI Global, 2011.

Lyon, D. (2018). The culture of surveillance. Cambridge: Polity Press.

McCourtie, S. D. (2020). Pandemic has forever changed online shopping, UN-backed survey reveals. UN News. October 08. Available at: https://news.un.org/en/story/2020/10/1074982 (Retrieved on December 31, 2020).Mellet, K., & Beauvisage, T. (2020). Cookie monsters. Anatomy of a digital market infrastructure. Consumption Markets & Culture, 23(2), 110–129.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29.

Narayanan, A., & Shmatikov V. (2008). Robust de-anonymization of large sparse datasets. www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

Nguyen, T., & Li, E. P. (2010). Online consumer privacy 2.0. Advances in Consumer Research, 37, 873.

Orwell, G. (1948/2014). 1984. Toronto, ON: Harper Perennial Classics. Available at: https://www.amazon.com/1984-George-Orwell/dp/1443434973

Peng, X. (2020). The Health QR Code is very useful for prevent and control the COVID 19 Pandemic in urban areas. People's Daily Online. August 17. Available at: http://paper.people.com.cn/rmrbhwb/html/2020-08/17/content_2003592.htm (Retrieved on December 14, 2020).

People's Daily. (2021). Over 70% of Chinese people increasingly use moneyless payment applications for their daily purchases in 2020. People's Daily. January 14. Available at: http://paper.people.com.cn/rmrb/html/2021-01/14/nw.D110000renmrb_20210114_2-07.htm (Retrieved on February 13, 2021).

Rose, N. (1999). Powers of freedom. Cambridge: Cambridge University Press.

Rose, N. (2001). The politics of life itself. Theory, Culture & Society, 18(6): 1–30. Schau, H. J., & Gilly, M. C. (2003). We are what we post? The presentation of self in personal webspace. Journal of Consumer Research, 30(4): 385–404.

Sparrow, E. (2014). Global information society watch. Accessed 25 February 2021, https://www.giswatch.org/thematic-report/internet-rights/digital-surveillance.

Taylor, D. (2009). Normativity and normalization. Foucault Studies, 7: 45–63.

Tencent Cloud Community. (2020). What is the mechanism of the Health QR Code? How accurate can it be? Netizens: what about privacy? Tencent Cloud Community. April 10. Available at: https://cloud.tencent.com/developer/news/608449 (Retrieved on December 25, 2020).

Tencent News. (2021). The birth of the Health QR Code: developed within 48 hours and promoted nationwide within 40 days. Tencent News. January 11. Available at: https://new.qq.com/omn/20210111/20210111A0B1QN00.html (Retrieved on February 14, 2021).

Tencent Technology News. (2020). Tencent Health QR Code used for over 1.6 billion times. Tencent Technology News. March 10. Available at: https://tech.qq.com/a/20200310/016327.htm (Retrieved on February 05, 2021).

Yu, J. (2021)., (2021, March 26). The ongoing digitalisation in China makes [Chinese] cities smarter. People's Daily. March 26. Avaliable at: http://house.people.com.cn/n1/2021/0326/c164220-32061447.html (Retrieved on May 15, 2021).

Wang, Y. (2020). The Health QR Code makes cities vivid again. (2020, 22nd March). The Chinese Communist Party News. March 22. Available at: http://cpc.people.com.cn/n1/2020/0322/c431601-31643030.html (Retrieved on December 10, 2020).

Zhao, H. (2020). The data collection and personal information protection in Heath QR Code. Procuratorial Daily. 10 June. Available at: http://newspaper.jcrb.com/2020/20200610/20200610_007/20200610_007_1.htm (Retrieved on December 17, 2020).

Zhao, X., & Belk, R. W. (2008). Politicizing consumer culture: Advertising's appropriation of political ideology in China's social transition. Journal of Consumer Research, 35(2), 231–244.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: Public Affairs.