Economy and Society

ISSN: 0308-5147 (Print) 1469-5766 (Online) Journal homepage: https://www.tandfonline.com/loi/reso20

Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China

Brett Aho & Roberta Duffield

To cite this article: Brett Aho & Roberta Duffield (2020) Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China, Economy and Society, 49:2, 187-212, DOI: 10.1080/03085147.2019.1690275

To link to this article: https://doi.org/10.1080/03085147.2019.1690275

Economy and Society Volume 49 Number 2 2020: 187–212
https://doi.org/10.1080/03085147.2019.1690275

Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China

Brett Aho and Roberta Duffield

Abstract

Technology giants, bolstered by weak regulatory oversight, have expanded capacities for personal data collection and analysis. This has resulted in a new set of power dynamics and logics of accumulation collectively referred to as surveillance capitalism. In response, the EU and China have adopted major policies on big data with implications for future social and economic development. Europe's General Data Protection Regulation is a reactive response, asserting individual privacy and placing limits on corporate use of personal data. In contrast, China's social credit system is a proactive response, combining surveillance architectures and AI technologies for purposes of statecraft. Using a comparative approach, this paper analyses the social and economic implications of two societies attempting to move beyond surveillance capitalism.

Keywords: surveillance capitalism; social credit system; GDPR; data privacy; big data; data regulation.

Brett Aho, Department of Global Studies Department, University of California Santa Barbara, Santa Barbara, 93106-7065, CA, United States. E-mail: brettaho@ucsb.edu
Roberta Duffield, Department of Global Studies, University of California Santa Barbara, Santa Barbara, 93106-7065, CA, United States. E-mail: rduffield@ucsb.edu

Introduction

In recent years China and the European Union have each adopted major policies on big data, placing their digital economies on two fundamentally different paths of development. In China, the social credit system (SCS) is being cultivated as one of the most substantial social and economic reform projects in national history and is expected to emerge as a defining institution shaping China's continued development in the information age. In Europe, the General Data Protection Regulation (GDPR) has been formulated as a comprehensive regulation on data protection and privacy, defining the way that both companies and states are able to collect and use data. This paper proposes that each governance project represents a radically different approach as to how data are conceptualized, with substantial implications for future social and economic progress. China's SCS has been in development since 2014 and aims to have most of its basic structures in place by 2020, whilst the GDPR was proposed in 2012 and adopted by the European Parliament in 2016, with most provisions entering into force in 2018.

This paper asserts that both the GDPR and the SCS have emerged in response to the globalized expansion of a relatively new logic of accumulation that scholar Shoshana Zuboff (2015, 2019) refers to as 'surveillance capitalism'. In brief, technology corporations, bolstered by a dearth of regulatory oversight, have gradually expanded their capacities for data collection and analysis as more and more human activity has moved online. Empowered by new algorithmic technologies, these corporations have developed capacities to mine vast databases of behavioural data, transforming individuals into data subjects whose actions, decisions and attitudes can be understood and manipulated for profit. This has resulted in a situation where a relatively small number of corporations now wield a substantial degree of power over the social and economic behaviours of consumers and populations around the world. This is the context in which both China's SCS and Europe's GDPR have emerged.

Although at first glance it may seem that the act of comparing these two policies represents a folly of apples and oranges, SCS and GDPR can be interpreted as concrete steps that each government has taken in response to the proliferation of data surveillance infrastructures. In a sense, they represent more than the policies that they inscribe on society and can be seen as broad normative statements on how each governing entity conceptualizes big data and how its associated technologies should be harnessed or restrained. Both governance projects represent assertions of state control over digital sectors, and both fundamentally alter the shape and course of digital economic development. Two very different futures emerge, with the European Union attempting to limit the power of surveillance capitalism with the passage of the GDPR, and China fully embracing its logics for further state use. The implications of these steps are substantial, placing Europe and China on very different paths in terms of social and economic development. In effect, what is emerging is two dissimilar forms of capitalism, operating on fundamentally different sets of logics.

The paper will begin by examining theories of surveillance capitalism, exploring how big data has the potential to shape modern society. Section three introduces the SCS – its political background and ambitions for restructuring the Chinese economy. The fourth section addresses GDPR and the EU, examining the political will behind its development, as well as what it means for the European tech sector. Finally, the paper concludes with a comparative analysis of potential social, political and cultural implications that these two governance strategies may pose. In terms of approach, this paper follows the notion of co-production, broadly examining how big data technologies have reordered societies, and how societies are pushing back to reorder these technologies in turn (Jasanoff, 2005).

Big data and the logics of surveillance capitalism

The rapid adoption of digital technologies has led to the production of massive troves of data by humans simply carrying out day to day activities. With every text and e-mail, every social media post, every website visit, every click or swipe, every song listened to, video watched, item purchased, game played, bill paid, place visited or medical symptom researched, behavioural information is now collected and stored. Massive databases have emerged, containing personal data on billions of individuals that can be analysed, studied and instrumentalized to modify future human choices. Tech firms have been amongst the first to embrace these possibilities, selling data and behavioural predictions to commercial ventures and advertisers, who in turn harness these insights to more effectively market products to consumers. Zuboff (2015, 2019) refers to this new structure of consumer relations as 'surveillance capitalism', arguing that data-driven consumption operates on fundamentally different logics than traditional market capitalism, in large part due to its propensity to anticipate and modify human behaviours. Karl Polanyi (2001[1944]) suggests that industrial market capitalism is largely based on the construction of three 'fictional commodities' in which human life is reframed as labour, nature is reframed as real-estate, and exchange as money. Zuboff (2015) builds on this conceptualization, suggesting that surveillance capitalism has reframed a fourth fictional commodity; reality itself. As she elaborates:

> Now 'reality' is subjugated to commodification and monetization and reborn as 'behavior.' Data about the behaviors of bodies, minds, and things take their place in a universal real-time dynamic index of smart objects within an infinite global domain of wired things. This new phenomenon produces the possibility of modifying the behaviors of persons and things for profit and control. (Zuboff, 2015, p. 85)

By reducing humans into quantified subjects and applying a scientific approach to the study of human behaviour, big data has made humanity more legible than

it has ever been before. As proposed by James C. Scott (1998), if something can be rendered legible, it can also be manipulated. In examining the foundations of past state endeavours to harness the power of data to implement utopian social projects, he identifies four key elements:

> the legibility of a society provides the capacity for large scale social engineering, high-modernist ideology provides the desire, the authoritarian state provides the determination to act on that desire, and an incapacitated civil society provides the leveled social terrain on which to build. (Scott, 1998, p. 5)

In the case of surveillance capitalism, big data provides the capacity, shareholder value provides the desire, powerful firms provide the determination to act on that desire, and an unwitting or indifferent populace provides the levelled social terrain on which to build. Within a milieu of deregulation, where corporate actors have become the dominant power exerting influence over social forces, high modernism has become privatized, motivated not by a utopian ideal, but by the generation of profit.

Zuboff uses the term 'extraction' to describe the relationship between corporate entities and individuals under surveillance capitalism, describing a process by which data are mined from a population, then analysed, operationalized and deployed to shape or modify behaviour (Zuboff, 2015, p. 2019). Data collection capacities have expanded dramatically by normalizing the amount of personal information that citizens share, and through the application of powerful algorithms, firms are often able to better understand and predict individual behaviour than individuals themselves. Today, applications are developed and tweaked using extensive A/B testing that seeks to maximize the time individuals spend on apps, as well as the breadth and depth of information that is disseminated and collected (Christian, 2012). In a TED talk entitled 'How a handful of tech companies control billions of minds every day', former Google design ethicist Harris (2017) stresses that firms are effectively hijacking human brain activity for profit. Indeed, the work of corporate data scientists is largely to understand and learn how human-technology interactions can be more effectively manipulated. As Nicholas G. Carr (2011) describes, on a neurobiological level, the human brain itself is becoming the subject of profit maximization strategies as human-technology interaction becomes increasingly integrated into daily life.

This is not to suggest that technology has transformed the individual into a mindless automaton whose free will has been subjugated by algorithms controlled by data operators. However as more and more aspects of human life continue to move from the analogue to the digital, it is important to consider that most digital interfaces are being developed by corporations whose motivations are first and foremost profit-driven (Alaimo & Kallinikos, 2017). As 'nudge' capacities increase, these interfaces are increasingly designed with behavioural modification in mind, with substantial implications for power relations within modern capitalism (Rouvroy, 2012). As Zuboff (2015) notes,

> False consciousness is no longer produced by the hidden facts of class and their relation to production, but rather by the hidden facts of commoditized behavior modification. If power was once identified with the ownership of the means of production, it is now identified with ownership of the means of behavioral modification. (p. 82)

This power over the means of behavioural modification is precisely what China seeks to harness in its development of SCS, and what Europe seeks to challenge in its adoption of the GDPR.

The rise of surveillance capitalism can be largely connected to the neoliberalization of political and economic structures as witnessed in the Atlantic region during the latter half of the twentieth century (Zuboff, 2019). Having come of age during an era of growing global free-market hegemony, Silicon Valley and the wider Western tech sector has emerged as one of the least regulated industries in modern history relative to its size. This is compounded by the fact that most existing regulatory institutions are simply not designed to respond to the challenges of the information economy, having been conceptualized in an era when industrialism was the primary driver of development (Cohen, 2016). As a result, most major technology companies have been allowed to operate free from state oversight, enabling the development of surveillance and social engineering capacities that might otherwise raise the alarm of state regulators.

As information technologies have begun to push civilization towards new forms of capitalist relations, at least two governments have made moves to assert some control over the ways that these technologies impact their societies, demonstrating a certain democratic (European Union) or authoritarian (China) self-determination over the forces of unrestrained techno-capitalism. In much of the rest of the world, including the United States, business models premised on mass data surveillance seem to be expanding. Even in the wake of the Cambridge Analytica scandal and foreign interference in the 2016 presidential election, the United States has yet to adopt any substantial data privacy laws at the federal level. Rather, surveillance capitalism as a new mode of accumulation has begun to permeate through a range of industries, including the finance, insurance, automotive, retail, and travel industries (Zuboff, 2019). With the considerable lobbying power of the tech industry, and the considerable profit-maximizing potential that surveillance-centred business models provide to other industries, it will be difficult for liberal market economies to regulate firms' use of data. Indeed, in much of the world, a sort of social contract seems to have emerged in which citizens tacitly accept data surveillance as long as firms continue to provide desirable services. In less developed countries, the focus of major corporations seems to be on securing new sources of data extraction, perhaps best exemplified by Facebook's controversial 'Free Basics' programme (Hempel, 2018; Yim *et al.*, 2017).

Scholars tend to form similar predictions around how unregulated tech sectors will gradually reshape societies. Columbia law professor Wu (2010) predicts an expansion of cartels and monopolies. Similarly, scholars Mayer-

Schönberger and Ramge (2018) argue that power will become concentrated amongst those companies that control the most valuable data. Historian Yuval Noah Harari (2018) concurs, asserting that regulation of the ownership of data is the key to preventing the concentration of wealth and power amongst a small elite. In the field of surveillance studies, scholars often highlight how asymmetrical data accumulation dispossesses subjects of agency over their personal information, laying the foundation for unjust data practices, including social sorting and discrimination (Cinnamon, 2017; Lyon, 2007, 2003). Most seem to agree that barring some form of political intervention, surveillance capitalism will continue to exacerbate trends of rising social and wealth inequality.

However, China's adoption of the SCS and the European Union's adoption of the GDPR have placed each state on a different path. In the case of China, the general aim is to transfer the power of data surveillance from the private sector to the public sector, repurposing existing surveillance infrastructures and technologies to advance state agendas. In Europe, the GDPR reflects broad normative aims to protect individual privacy and preserve individual freedom, consequently limiting the degree of behavioural control that corporations can exert over consumers. The next two sections will examine the SCS and the GDPR in turn. In the final section, the implications of these two paths will be examined.

China's social credit system (SCS)

Background

China is currently in the process of developing 'the boldest and most ambitious governance reform programme launched by China since 1978' (Sapio, 2017). Political scientist Sebastian Heilmann (2016) refers to the project as establishing a 'new digital Leninism', describing SCS as the 'the most ambitious Orwellian scheme in human history, seeking to establish an all-seeing state' (p. 17). The project builds off the fundamental logics of surveillance capitalism as well as its technological infrastructures, expanding upon the surveillance and social engineering capacities whilst harnessing their potentials for purposes of statecraft. The foundation of the project is the assignment of dynamic credit scores for every economic actor operating within the national market, from giant conglomerates and state-owned enterprises down to small businesses and individuals. These scores are assigned by a series of algorithms operationally managed by central government authority and allow the state to encourage desired social and economic behaviours whilst discouraging undesirable behaviours through an operationally managed system of tailored rewards and punishments. What emerges is a novel system that enables data-informed economic and social planning on a national scale.

The root of the SCS lies in the rapid digitization of the Chinese economy. According to official statistics, in 2017 China was home to 731 million internet users and 695 million mobile internet users, and Chinese consumers are now responsible for 40 per cent of the value of all global e-commerce transactions (CNNIC, 2017; Woetzel *et al*., 2017). As headlines in the *Financial Times* have declared: 'China's digital economy is a global trailblazer' (20 March 2017); 'China gears up for leap into digitization of industry' (19 December 2017), 'China mobile payments dwarf those in US as fintech booms, research shows' (23 February 2017). In light of the rapid digitization of the Chinese economy, computer scientist Kai Fu Lee (2018) describes China as the 'Saudi Arabia of data', referring to the unparalleled amount of data that Chinese citizens produce every day. He argues that the depth of digital integration in China is unmatched in the rest of the world, as mobile payments replace hard cash for most daily economic transactions, and apps such as WeChat become central features in everyday social and economic life. As smartphones have made everyday life legible through the technological architectures of surveillance capitalism, the Chinese state now seeks to use these capacities as a new source of power and control.

Ideological foundation

State surveillance has a substantial history in modern China, and the development of the SCS is not without precedent. In the wake of the 1949 revolution, all Chinese citizens were organized into a *danwei,* or work unit, which served as an early form of government surveillance and control over the personal lives of individuals. These administrative formations were responsible for state oversight over a wide range of everyday human activities, including travel, marriage, housing, education, population control and health care. The *danwei* served as the primary tool by which the Communist Party of China (CPC) sought to organize the economic ambitions of Mao's Great Leap Forward, and any dissent to the Party's vision was recorded in a *dang'an*, a government file for maintaining personal records on Chinese citizens. However, a tradition of social governance in China stretches back further. In his study of social governance in China, scholar Bray (2005) advocates for a genealogical method, which highlights a complex process of layering in which seemingly disparate practices from the past come together to explain the development and emergence of a modern system. In this regard, elements of the SCS can be interpreted as modern reflections of a range of surveillance and control policies evident throughout China's dynamic past, from practices of Confucian bureaucracy, to the social policies of the Yan'an Rectification Movement and the influence of Soviet planning advisors in the 1950s.

Although the *danwei* still exists, it is only a single piece of a much more profound surveillance society that has more recently emerged in China. Surveillance and censorship policies, commonly referred to as the Great Firewall of

China, have been part and parcel of the Chinese internet since its inception. In public spaces, China is currently in the process of building the world's biggest camera surveillance network equipped with facial recognition technology, with 170 million CCTV cameras installed by 2017, and an estimated 400 million more to be running by 2020 (BBC News, 2017). If a particular group is deemed a security risk, coercive surveillance is intensified, as exemplified by the ongoing securitization of Xinjiang and its marginalized Uighur population (Mitchell & Diamond, 2018). A perceived deficit of social trust has contributed to the expansion of Chinese surveillance capacities, whilst a culture of informing on one's neighbours remains widespread (Hawkins, 2017; Lubman, 2017). In this context, public support for the SCS and its surveillance imperatives remain high, and it is broadly regarded as a way to bring about a more honest and harmonious society (Kostka, 2018).

Much of the impetus for the SCS's development stems from a historical lack of trust between economic actors in China, alongside weak institutions that have struggled to rein in unsustainable and corrupt business practices (Dai, 2018). In development discourse it has become common to acknowledge effective institutions as important drivers of economic growth; over the past two decades, China's rapid economic development has largely outpaced its growth in institutional capacity (Ezrow *et al.*, 2016; Nederveen Pieterse, 2015). As a result, many laws and regulations concerning economic activity in China remain poorly and selectively enforced across a range of industries (Zhang & Zhang, 2016). The core concept SCS strives to impose is 'self-regulation of enterprise' in which businesses comply with laws and regulations of their own accord, thereby easing the burdens on existing enforcement and compliance structures (State Council, 2017). Hence, the SCS is being implemented as a way to complement the ultimate functions of other institutions by shaping individual and firm behaviour, ensuring compliance with government laws and regulations and incentivizing corporate social and environmental responsibility. In one regard, the SCS represents a means to reconsolidate control in the face of weak institutions, representing a creative and novel enforcement mechanism that, rather than strengthening existing institutions, diminishes their importance.

A panopticon with Chinese characteristics?

As the Chinese State Council's Planning Outline notes, the goal of the system is to 'broadly shape a thick atmosphere in the entire society that keeping trust is glorious and breaking trust is disgraceful, and ensure that sincerity and trustworthiness become conscious norms of action amongst all the people' (State Council, 2014). By achieving extensive surveillance and control over social and market behaviours, the SCS seeks to ensure good behaviour between economic subjects, as well as compliance with regulations and participation in government agendas. The behaviour of subjects is controlled not by means of force,

but by incentivizing good behaviour and encouraging voluntary compliance and participation in state programmes and policies – the self-regulation of the SCS vision. In many ways the SCS can be viewed as a system of behavioural control whose functionality is based on principles of coerced self-regulation first presented in Jeremy Bentham's (2009 [1791]) panopticon proposal, in which subjects are instilled with the perception of constant surveillance through the power of architectural design, thus altering their behaviour not through force, but through a form of psychological manipulation. Whether the subjects are criminals, consumers or corporations, under the watchful eye of Big Brother, self-regulation of behaviour ensues. Just as Bentham's panopticon increases the effectiveness of the prison whilst reducing the number of guards, the SCS represents a means for increasing the efficiency of state institutions, whilst dispensing with the need for expanding institutional personnel.

As noted, the SCS functions primarily based on a dynamic system of rewards and punishments tied to credit scores. As the CPC's Planning Outline (2014) lays out, 'the mechanisms encouraging trustworthiness and punishing untrustworthiness function directly on the credit conduct of all societal entities, and are the core mechanisms for the operation of the social credit system'. 'Trustworthiness' is established through SCS scores, and rewards and punishments are developed by authorities with the aim of addressing and mediating the specific problems present within a population, sector, industry, firm or region. Whilst some carrots and sticks may be universal across all contexts, others will be carefully tailored for specific populations, industries or regions. Some of the rewards and punishments that have been outlined within the Planning Outline and existing literature on SCS are identified in Table 1.

What emerges is a system that allows a government an unprecedented degree of control over the behaviour of both firms and individuals within its territory. Zuboff (2015, 2019) argues that the architecture developed under surveillance capitalism makes Bentham's panopticon seem prosaic, referring to these power structures in the hands of corporations as the Big Other. However, by transferring these powers back to the state, Big Brother is reborn, creating a society where 'habitats inside and outside the human body are saturated with data and produce radically distributed opportunities for observation, interpretation, communication, influence, prediction and ultimately modification of the totality of action' (Zuboff, 2015, p. 82). This however is not to say that SCS will rapidly transform China into a high-tech totalitarian dystopia; sensationalist allusions to George Orwell's 1984 exaggerate the system's potential and misinterpret the CPC's intention. Rather, the system should be seen primarily as an innovative means to compensate for weak institutions and to increase statecraft efficiency. Given the SCS's ability to be monitored and adjusted in real-time thanks to digital data collection, the system will provide the Chinese state with the ability to roll out new policies and programmes at speeds unparalleled in any other country. Government agencies can thus quickly observe the effects of their policies and interventions and adjust accordingly to maximize effect, enabling a process of rapid regulatory learning.

Table 1. A system of carrots and sticks.

Individual Rewards	*Individual Punishments*
Lower tax rates	Travel restrictions
Discounts on utilities	Blocking purchases of train/plane tickets
Deposit-free rentals	Visa restrictions
Lower interest rates	Hotel restrictions
Faster check-in at hotels and airports	Throttled internet speeds
Faster internet speeds	Restricted access to higher education
Increased access to public services	Job restrictions
Discounts on public transportation	Public shaming and blacklisting
Faster processing of travel visas	Credit restrictions
Shorter wait time at hospitals	Higher taxes and loan interest rates
Increased visibility on dating apps	Restrictions on property ownership
Firm Rewards	*Firm Punishments*
Commendations and positive publicity	Warnings
Removal of red tape and reduction of state regulation	Blacklisting mechanisms
Access to markets for public services	Market withdrawal and shutdown of e-commerce accounts
Preferential bidding on public contracts	Circulation of criticism to business partners
Granting of accreditations and qualification certifications	Public shaming/censure
Policy support	Red tape and increased administrative burdens
Administrative approvals	Unfavourable loan conditions
Tax incentives	Higher taxes than compliant competitors
Access to preferential credit services	Restrictions on stock or bond investments
Access to investment opportunities	Decreased opportunity to participate in publicly funded projects
Open markets and unrestricted foreign investment opportunities	Mandatory government approval for investments, even in sectors where market access is not usually regulated
Expedited processing of permits and visas	Managers denied tickets for high-speed rail or international business flights

Source: Hvistendahl, 2017; Meissner, 2017; Sapio, 2017; State Council, 2014.

To demonstrate the functional capacities that the SCS provides to Chinese authorities, one need not look further than the system's ability to address China's environmental problems. Today, China's urban landscapes are amongst the most polluted in the world. China policy expert Elizabeth Economy (2007) refers to this growing environmental crisis as the 'great leap backwards', as widespread soil, air and water contamination have led to substantial public health dilemmas. With energy consumption and vehicle use continuing to rise, environmental issues will only proliferate as China reaps the consequences of its industrial and economic success. As Nederveen Pieterse (2015) notes, 'Pollution incidents going back to the 1980s reveal the contradictions between growth and development. The loss incurred as a result of

pollution each year is 10% of same year's added GDP and is likely to rise higher in 2020' (p. 1989). For these reasons, the amelioration of environmental concerns is amongst the early aims that SCS has forwarded.

Much of the difficulty China faces in the environmental arena stems from poor enforcement of pollution regulations, corruption and feeble institutions disincentivizing firm compliance (Eaton & Kostka, 2017; Wang *et al.*, 2003). Again, much of SCS's power lies in its ability to bypass institutional weakness and coerce economic actors into self-regulation. The Planning Outline (2014) proposes new state capabilities for ecological monitoring through establishing 'credit evaluation structures for enterprises' environmental behavior'. Former head analyst at the Mercator Institute for China Studies Mirjam Meissner (2017) notes that the government's current goals include the development of a system able to carry out real-time emissions and energy consumption oversight of polluting industries using sensors in chimney stacks and smart metres. Pilot projects have already been launched, such as Green Horizon which monitors and responds to Beijing's pollution spikes with real-time measures for traffic and industries (Cooper, 2016).

Besides immediate regulatory enforcement, SCS also incentivizes business participation in initiatives designed to improve performance over longer periods of time. For example, firms that voluntarily reduce energy consumption or carbon footprints may see credit scores improved and rewards such as decreased tax rates. Because different places and industries face their own unique set of environmental problems, programmes can be tailored to local specifics. For example, increased water consumption penalties may be levied against industries in water-scarce areas as compared to regions where supplies are bountiful. SCS incentives could even theoretically promote positive competition between firms. Nor does regulation stop at environmental concerns; the same principles of bespoke monitoring and coordination exist for any other category of economic interest, such as corporate social responsibility, consumer satisfaction, product output and so on.

Given the large volume of data collected, SCS could eventually reach deep into the lives of citizens and provide a range of policy insights related to the well-being of citizens and employees. For example, a firm's occupational health practices could be measured through the number of transactions that employees make at medical establishments. High workforce spending on medicine and healthcare may serve as an indicator of poor occupational health practices and the social credit score of the unhealthy enterprise reduced accordingly. To raise the score, the firm would be incentivized to adopt policies that improve relevant working conditions, and the success of those policies could be analysed in real-time by continuing to monitor employees' medical transactions. Furthermore, through surveillance of personal communication and social media, digital algorithms could theoretically measure the attitudes and mental health of workers, enabling the creation of complex metrics that could potentially revolutionize labour relations and human resources practices. The potentials for firm

regulation are virtually limitless within a system that permits unrestricted surveillance and intervention.

From surveillance capitalism to a planned economy

In many regards, the emergence of surveillance capitalism and subsequent development of SCS has laid the groundwork for a revival of the Chinese planned economy in a new and improved hybrid form. One reason that state planning in the twentieth century largely failed was because executive powers lacked both the data and the data processing tools necessary to adequately control something as large and complex as a national economy (Harari, 2016, chapter 11). In the heyday of Soviet-style central planning, the technology simply did not exist to allow governments to adequately steer their countries in a tumultuous sea of complex geopolitical interactions. However, modern digital technology is ripe for a country to once again experiment with high modernism's proclivity for social legibility. As Chinese billionaire Jack Ma Yun, founder of the Alibaba Group notes:

> Over the past 100 years, we have come to believe that the market economy is the best system, but in my opinion, there will be a significant change in the next three decades, and the planned economy will become increasingly big. Why? Because with access to all kinds of data, we may be able to find the invisible hand of the market. (*Global Times*, 2017)

This return to economic planning can trace its roots to the emergence of systems engineering as an interdisciplinary field of study. As commentator Hvistendahl (2018) observes, interest in systems engineering has waned in Western education and industries but has exploded in China to the point where today it is a mandatory subject for all students at the CPC's Central Party School in Beijing. The centrality of systems engineering in CPC planning is particularly visible in the policy prescriptions laid out by Xi Jinping, who noted in 2013 that 'comprehensively deepening reform is a complex systems engineering problem' (Hvistendahl, 2018). Systems engineering approaches lie at the centre of the SCS and will be used to continually develop the networks as well as the policies and programmes embedded within it. In the eyes of the CPC, the economy represents the mother of all systems, which, with enough data points, can be studied, manipulated and understood. Recent developments in machine learning represent the primary technological developments that have made it possible for China to use big data and the SCS as a means of steering economic growth.

With huge amounts of data, real-time feedback and machine learning algorithms that can process and understand outputs, the SCS presents the CPC with an instrument that can help the party respond to the fluctuations of the market almost instantaneously. Using the SCS, economic planners now have

the potential to direct firm behaviours by changing rewards and punishments to fit shifting global economic environments. In moments of economic downturn, the SCS might be tweaked so that businesses face fewer punishments. In a similar way, rewards can be offered as a form of economic stimulus. If the system finds that a light touch is preferable to a heavy hand, policies of virtual deregulation can also be prescribed and implemented. These micro-interventions may be tailored to individual industries and can be coordinated across the entire economy. With every intervention and tweak of the SCS, massive amounts of data are collected and analysed in order to understand both the seen and unforeseen consequences of the action, thereby improving the project's grasp of the economy as a system, and the ability of planners to implement more effective actions in the future. The longer that the system is in operation, the more effective it becomes.

Europe's general data protection regulation (GDPR)

Background

On 25 May 2018 the GDPR was formally implemented, ending a two-year transitional period that followed the regulation's final adoption in April 2016. GDPR has been heralded as 'one of the most robust data privacy laws in the world' that sets a new global standard for data collection storage and use (Pardes, 2018). Its twofold aim is to 'enhance data protection rights of individuals and to improve business opportunities by facilitating the free flow of personal data in the digital single market' (Council of European Union, 2015, p. 1). By unifying digital protection practices, the general goal is to enhance the degree of control that ordinary citizens have over their personal data, as well as how it is collected and used in an age of data-driven capitalism. Substantively, the regulations place meaningful limits on how corporations can collect and use personal data, effectively hindering the practices of surveillance capitalism.

GDPR replaces the Data Protection Directive 95/46/EC (DPD) introduced in 1995 to unilaterally standardize the multitude of extant data protection laws within each EU nation, in turn based upon an older set of principles known as the Fair Information Practices. DPD's primary objective was to uphold the protection of the individual with regards to the processing of personal data and its free movement. The shifting technological landscape soon outstripped DPD's oversight capabilities, creating legislative gaps and fragmentation. In addition, its directive status allowed individual member states to differentially interpret and modify the original edict with supplementary national laws. As a result, data regulation in Europe has previously been uneven, such that businesses operating across borders in the EU's single market found themselves navigating an increasingly complex legal framework. In response, a proposal for new regulatory legislation on digital data protection was issued in January 2012, paving

the way for what would eventually become the GDPR (Pardes, 2018; Ryz & Grest, 2016; Tankard, 2016).

GDPR's implementation involves a reimagination of geographical borders to match a new digital imaginary. The regulation applies to all individuals within the EU and European Economic Area, regardless of nationality or origin. Controllers and processors of personal data located outside the EU are also subject to GDPR if their business practices involve the data of any EU individual or entity (Ryz & Grest, 2016). In the case of the United Kingdom, royal assent for a new Data Protection Act was granted in May 2018 that allows for a continuation of the GDPR in a post-Brexit nation (Burgess, 2018).

Ideological foundations of the GDPR

Individualism is considered a major component of the political ethos found in many modern, affluent Western societies (Halman, 1996). Within the liberal democratic state, a citizen's day-to-day decisions and preferences are based primarily on the realization of personal interests, and one of the chief roles of the state is as protector of individual freedoms. The liberal ideology of the inviolability of the individual can trace intellectual roots back to the Renaissance and the Reformation. During the Enlightenment era of the late seventeenth and eighteenth centuries in western Europe and beyond, thinkers such as Voltaire, Rousseau, Locke, Hume and Kant further developed the concept of personal liberty which would come to have a profound effect upon Western political, social, economic and cultural practices. The ideology of liberalism crystallized around the idea of a society based on natural law over prejudice, privilege and tyranny; reason and secularity over faith; the inherent goodness of man; tolerance; and the state as an instrument of ever-evolving progress. Philosopher John Locke outlined the place of the individual within this as defined by the social contract; a cooperation between citizen and government safeguarding a functioning society and the personal rights of its constituents through representation and the rule of law.

The state ethos and governing principles within the constituent nations of the contemporary European Union cannot be said to share a blanket political-philosophical homogeneity. However, broadly speaking, the preservation of the individual and their rights is represented in multifaceted forms of legislation, governance, behaviour and culture throughout the region (Halman, 1996). This is not to say that the Union is immune from infringement on these values, nor impervious to crises. Nor is it to proclaim the superiority or indelibility of the philosophically liberal founding credentials of its constituent nations. Indeed, in many Global North liberal market economies, the growing illegitimacy of inert political classes held hostage to big business and self-interest are characteristic of the paradox of the post-democratic moment (Crouch, 2016; Nederveen Pieterse, 2018). However, what is significant is the attempt, at least, to embed the values of respect for human dignity, liberty and equality within the

European Union's language and ideological framework, reflecting the basic tenets of Enlightenment and humanist thinking (Kaili, 2016). This can be seen as both a continuum of a collective socio-political disposition, and a reflexive response to growing awareness of data misuse, thrown into relief by high profile cases such as Cambridge Analytica and the NSA spying scandals.

An affirmation of digital privacy and individual rights

Although the simplification of regulations for businesses is a substantial motivation for the development of the GDPR, at the core of the legislation is a reaffirmation of the rights of the individual as the prime unit through which liberty is expressed. Indeed, GDPR has been variously described as a 'noble and essential' law to 'protect personal data seen as attributes of the individual … and reclaim our rights and freedoms' (Maurel & Aufrère, 2018). Chief cybersecurity strategist Tom Pendergast portrays GDPR as the latest move in the 'new Cold War over data protection' where personal information is the 'currency of the modern age'. In his words:

> Vying against each other are those societies that believe that individuals have an absolute right to control their personal data – to exercise the same kind of dominion over data that they do over their bodies or their personal property – and those that believe that personal data is a good to be traded on the open market and thus subject to the same market forces at play elsewhere … *The EU stands firmly for the interests of the individual.* (Pendergast, 2018, emphasis added)

Indeed, GDPR can be seen to take on a semi-messianic role, with pundits asking questions such as 'will the spring of 2018 be remembered as the time when the right to privacy was enshrined as a fundamental human right?' (Pendergast, 2018). This rhetoric is perhaps reflective of the sea-change in the practices and principles of market economics that Zuboff (2015, 2019) maps out with regards to surveillance capitalism and its contemporary challenges to the modern liberal order.

The regulatory language of the GDPR does indeed seem to reflect this sense of urgency, solidifying the safeguarding of individual rights throughout its 99 articles. Under Articles 13 and 14 on the right to notification, all users must be informed of how their data are to be used and given the opportunity to opt in or out of the process (European Union, 2016). This consent must be given freely and unambiguously, without coercion or entrapment, disallowing such practices as the provision of extra services to those who agree to share personal information. In addition, no data may be transferred to third parties or outside of the EU without specific prior agreement of the involved parties (Ryz & Grest, 2016). Further, under Article 15 on the right to access, individuals now hold the authority to view information held on them and withdraw from data processing if they change their mind. The right to be forgotten has

also been reinforced, now requiring data controllers to remove information that is considered to be extraneous, inadequate or no longer relevant. These requirements will naturally require that data collecting entities exercise greater oversight over what information they hold, where it is held and how it is being used at all times. (Council of the European Union, 2015; Tankard, 2016).

Implicit throughout these terms is a notion of the individual as an active agent in determining their own positionality of self, where the 'right to explanation' or 'right to be informed' moves beyond mere passive 'data protection'. Data protection scholars Malgieri and Comandé (2017) argue that this significance arises from the nexus between the rights to access, notification and not to be subject to any automated decision-making made on a solely-algorithmic basis. Indeed, the inclusion of the latter precept is particularly telling when considered through the lens of Zuboff's (2015) re-conception of false consciousness as produced by hidden facts of commoditized behaviour modification. Implicitly, GDPR recognizes the shift in power she outlines from ownership of the means of production to commercially-driven data analytics and the role this technology plays in subject formation. Article 22(1) of the GDPR which governs the automation of data analytics states that:

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly *significantly affects him or her*. (European Union, 2016, emphasis added)

This is further support by Articles 13(2)(f) and 14(2)(g) which both state that:

> The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, *meaningful information about the logic involved*, as well as the *significance and the envisaged consequences of such processing for the data subject*. (European Union, 2016, emphasis added)

This clearly indicates a recognition of the potential ramifications of behavioural analytics upon the individual, whereby big data transcends the classification of mere 'technology' to embody a profoundly social intention. Specifically, this refers to the potentiality for profile-targeted marketing and 'nudge' economics to be used to exploit consumer vulnerabilities in order to mould purchasing attitudes, past the demographic grouping of traditional market research right down to the individual level. As established, 'oftentimes, these algorithms are not only unknown but also unintelligible by individuals' (Malgieri & Comandé, 2017), or even data controllers themselves. Machine-learning technologies only add further opacity. This is the black-boxing of the information civilization, where lack of regulatory oversight can be seen to have unwittingly constructed an architecture of unintelligibility and alienation from the self. This creates a paradox of transparency, where the question becomes not one of legibility, but of power – transparency, but for whom? If big data analytics can be seen

as the compulsion for market knowability, then it is only for the eyes of corporate elite interests. GDPR can therefore be seen as a reclamative response of transparency *for* the individual (by rendering visible and providing choice), but crucially not *of* the individual. As the epistemic contents of big data's black-box is revealed, this simultaneously re-privatises the personal lives of citizens, if they so choose it.

The right not to be subject to any automated decision-making made on a solely-algorithmic basis also has implications for the notion of consent that GDPR forwards. Automation serves to bypass human rationalities by transforming data from an abstract reduction to a rendition of human behaviour 'increasingly understood as approaching reality itself' (Chandler, 2015, p. 836). Jurist and technology research analyst Antoinette Rouvroy (2012) terms this the 'truth regime' of algorithmically generated insight that presents claims to pure factuality in yielding insights that appear to have always existed, but obscured beneath the chaotic surface of reality and the human fallibility of heuristic bias and emotion. GDPR can therefore also be seen as a reclamation of human agency from the post-human infallible authority of big data analytics, emphasizing the individual's integrity once more.

Safeguarding human agency: an architecture

At GDPR's core is the principle of 'data protection by design and by default' (European Union, 2016). This encapsulates a wholesale reorientation towards how data regulation have previously been conceived and enacted. Rather than viewing data protection as a consideration or compliance as in former legislative iterations, security is repositioned as the central function around how data are collected, stored and exploited by building it into its operative foundations (Zerlang, 2017). A base requirement to pseudonymize or anonymize all personal details is intended to protect subjects from being identified in the event of a data breach. Although these are prescriptive requirements, much of the GDPR elsewhere avoids rigidly defined details on how security goals are to be realized. This circumvents the risk of future obsoletion as technology changes and embeds longevity within GDPR's precepts (Tankard, 2016). The regulation's framework can therefore be considered a 'legibility-by-design system' which attempts to realize and enshrine individual autonomy within its architecture (Malgieri & Comandé, 2017).

Since GDPR is a regulation and not a directive like its DPD predecessor, it is directly binding for every member state without the need for national level approval or possibility of amendment. Any breaches of user privacy require the notification of EU data protection authorities within 72-hours of its occurrence. For those organizations that rely on significant data processing activity, they are required to employ a Data Protection Officer (DPO) independent of the business who will oversee GDPR compliance (Tankard, 2016; Zerlang, 2017). If a data processing initiative is considered to be high-risk regarding

its possible impact on the subjects involved, a data impact assessment and delineation of requisite safeguards will be required before analysis can move forwards. These measures also reaffirm the responsibility of data processors for the security of the information they hold (Ryz & Grest, 2016). Sanctions for non-compliance are stricter than under the DPD, with violators liable for fines of up to 4 per cent of total revenues or 20 million euros, whichever is higher, for serious breaches (Tankard, 2016). GDPR's reach is not exhaustive, however. Data processing without compliance is still permitted for matters of state security, justice and military matters; or data processing conducted by individuals or within a personal household, for example.

Implications, comparisons and conclusions

Given the transnational nature of the tech industry, these divergent policy regimes have already begun to come into contention. Concerns about data collection and surveillance practices lie at the centre of political spats, national security debates and trade disputes between Europe, the United States, China and beyond. A report from the NATO Cooperative Cyber Defence Centre of Excellence warns about the security threats posed by Huawei's 5G technology, citing Sun Tzu: 'the supreme art of war is to subdue the enemy without fighting' (Kaska *et al.*, 2019). US President Donald Trump explains that EU competition chief and tech industry regulator Margrethe Vestager 'hates the United States, perhaps worse than any person I've ever met' (Stevis-Gridneff, 2019). Citing the cases of Huawei, Google and Samsung, political scientist Abraham Newman (2019) describes how the United States and China have begun strategically weaponizing supply chains in what he describes as a new 'quiet war'. As digital technologies become tied with divergent models of social and economic development, it seems likely that data collection and surveillance will only continue to grow as a substantial component of ideological clashes.

The political will of the State Council to see SCS to completion is undeniable, drawing on China's industry advantages in surveillance and data collection. Yet, the ambitious infrastructures demanded by SCS are without precedent and must be built almost from scratch. Technological feasibility, bureaucratic barriers and parity of enforcement pose significant challenges to the CPC's grand vision of economic omniscience, particularly concerning information pipelines from rural areas and smaller towns where extant technology use and state oversight are weak. Data theft, fraud and the emergence of a shadow industry of loopholes is likely, spurred by fear of sanctions for non-compliance, or powerful private enterprises loath to share their valuable data assets with the state (Meissner, 2017). Even if correctly implemented on some scale, there is no guarantee that the system will be successful, or how disruptive the teething problems associated with the installation of a new regime of this scale will be. Despite the epistemic armour of the algorithmic truth regime, its insights do

not guarantee accuracy and remain dependent on the veracity and quality of data mined. Of concern too is state misuse of data, as raised above in the case of the marginalized Uighur population in Xinjiang and potentially on wider scales beyond. Big data surveillance enhances the capture and categorization of difference, breeding potential for systemic social polarization as human subjects are identified and sorted according to worth and risk (Lyon, 2003), as already evident by Mara Hvistendahl's (2017) account of a nascent digital underclass.

GDPR has fallen foul of similar logistical and operational pitfalls given its ambitious scope. By the European Union's own admission

> companies seem to be treating the GDPR more as a legal puzzle, in order to preserve their own way of doing things … rather than adapting their way of working to better protect the interests of those who use their services. (EDPS, 2019, p. 5)

Indeed, by the rules of the GDPR, the 'lead regulator' of multinational firms must be located in the county where firms have their 'main establishment', which for most large firms, including Google, Facebook, Twitter and Microsoft, is Ireland. Despite thousands of alleged data privacy violations, Ireland's Data Protection Commission has been slow to take enforcement actions, causing some to raise concerns about regulatory capture (Vinocur, 2019). This disparity between identification and action appears to be common across the EU, with reporting from the period of GDPR's inception in May 2018 until January 2019 indicating 59,000 data breach notifications but only 51 fines levied, mostly of low value (DLA Piper, 2019). However, despite the implementation challenges of GDPR and SCS, the direction of each policy regime is clear. As with any new governance paradigm, processes of regulatory learning will ensue, and each society is likely to continue progressing along prescribed trajectories towards the normative vision embedded within.

Economic implications

The economic ambition of the CPC's social credit system is clear – it is to be the powerhouse for growth that will deliver Xi Jinping's vision of national prosperity and influence. In order to achieve this, China must recentre its export-based economy to a development model based on consumption and quality rather than price competition if it wishes to secure sustainable, sensible economic practices (Nederveen Pieterse, 2015). In theory, SCS is geared to deliver an economy operating at its maximum potential in all possible contingencies through the exploitation of mass data collection, machine-learning algorithms and, eventually, real-time cybernetic feedback and adjustment. The eventual goal is a revival of the planned economy equipped for the information age, where big data and its analytics are tools for economic advancement, first and foremost. In essence, China is taking the architectures first developed under the guise

of surveillance capitalism and is re-tooling them to achieve their full potential under a new ambitious economic model.

GDPR too professes to provide economic benefits, based around the harmonization of data legislation between EU member-states that will free the union's single market from bureaucratic congestion. However, some experts warn that the regulation will have a chilling effect on the research and development of new big data and AI technologies (Ness & Chase, 2018). Many tech firms may be compelled to shift their investments to countries such as the United States, where big data operations can continue free from governmental oversight. However due to the legislation's opaque wording and many ambiguously defined terms within its text, the extent to which the GDPR impacts Europe's digital economy will be determined by courts and GDPR institutions such as the European Data Protection Board over the coming years (Ness & Chase, 2018). What is clear, however, is that the policy will fundamentally disrupt the course of surveillance capitalism in Europe.

Social implications

Despite the economic motivations outlined above, GDPR's rationale appears to be profoundly socially grounded. It is built around the notions of personal consent, empowerment through awareness, and an aversion to insidious processes of subject formation and behavioural modification as dictated by commercial interests. Central to this is the individualism that has characterized the nation-building projects and statecraft of western Europe, rooted in Enlightenment-era political philosophy and broadly speaking, informing the contemporary social order amongst EU populations. Fundamentally, GDPR is seeking to define the relationship between the individual and the digital in a way that protects personal autonomy and agency. SCS too recognizes the potentiality of behavioural modification, instead choosing to harness it to help bring about 'social harmony'. This can be explicit, as in the case of government regulation of a firm's commercial activity that can be redirected in order to meet a specific economic goal. However, it is also implicit, embedded within the surveillance and assessment of citizens' behaviour through individual credit ratings paired with social perks and punishments.

This differs from GDPR's notion of the individual in several key ways. Although the SCS and GDPR consider the behaviour of both the individual and the commercial entity, GDPR seeks to govern only the latter, whilst SCS extends control over both. Under SCS the individual is thus conceived of in terms of its worth as an actor in relation to the greater Chinese society and market – something which GDPR expressly desires to abandon. In doing so, GDPR invokes the presumed inviolability of personal rights and freedoms in its justification of regulation. Before condemning SCS's behavioural modification as the zombification of a population into economic pawns, Western liberal sensibilities must also consider the rationale behind SCS's perceived

social benefits, alongside (justified) fears of its appropriation as a tool of political repression. The rhetoric of individual sanctity may be missing within Chinese discourse, but not without reason. Instead, the transparency of the credit rating is framed as a trust-building exercise toward a 'harmonious society' with a 'sincerity culture' as its end goal (State Council, 2014). Surveillance is designed to breed self-regulation and the fulfilment of social harmony; for China, the path to attainment of individual well-being thus lies through the collective.

Both SCS and GDPR can thus be seen to profess the needs of its citizens, but realized through radically different paradigms and intellectual discourse around personal data analytics. Broadly speaking, the dichotomy of individual versus collective interest can be seen to inform this – a cultural dimension of difference between China and the liberal West already well-established. Indeed, in what may seem a curious twist of fate, one of the world's first big data projects, carried out by IBM Europe, analysed 116,000 employee surveys between 1967 and 1973 to develop a theory of cultural dimensions that quantifies China's collectivism versus Europe's individualism (Hofstede, 1983).

Political implications

GDPR can be read as Europe's challenge to trends of corporate consolidation of power accelerated by innovations arising out of an unregulated tech sector. At its core, it is an attempt to reassert democratic ideals within the European project in response to the changes to social consciousness posed by surveillance capitalism. It is a repudiation of corporate power in the name of human interest, with economic benefit seemingly taking second place to an ideological reassertion of individual rights as inherent to a just political system. China's SCS demonstrates a different sort of challenge to commercial agency. The SCS asserts the dominance of the state over private enterprise, seeking to co-opt economic activity within its bounds. This represents a re-establishment of control over national markets that were first opened up under the Deng Xiaoping premiership and policies of 'socialism with Chinese characteristics' (Leonard, 2012).

Both GDPR and SCS are formulated around the *longue durée*. China's SCS is envisioned as a substantial overhaul of the Chinese economy to refit it for the future, using digital data processing algorithms to formulate an optimal economic paradigm for China's future growth. GDPR too recognizes the centrality of these technologies to current and future societies, building mechanisms within its text to weather information technological advancement in the upcoming decades whilst considering a holistic view of the impact of surveillance capitalism on citizens' personal lives. However, this is where the two futures bifurcate. Whether one agrees with the moral implications or not, China's embrace of data surveillance represents their proactive march into the future. It is symptomatic of the long-term planning of a ruling party that approaches development through the lens of 'credibility and gradualism' as a mainstay of future success and policy (Ho, 2009). The CPC is formulated around 30-year planning cycles, where

one must dedicate a 50-plus year career to political service in order to advance to the upper echelons of the Party's hierarchy (Leonard, 2012; Li, 2013). The SCS represents the careful life work of experts in systems engineering, social psychology, computer science, artificial intelligence, economics, political science, and countless other fields. It is not the result of democratic will, but of cadres of highly-trained scientific minds seeking to apply their knowledge for the advancement of society as a collective project.

In contrast, GDPR is only reactive, playing catch-up to legislative fragmentation and data infringement scandals such as Cambridge Analytica. Although GDPR's attempt to forward personal rights is commendable (at least within the context of Western liberal thinking), when considered against its wider political and cultural context, the forecast is less certain. GDPR is highly significant, precisely because it stands alone as a bold move against plutocratic currents and corporate government. Its look to the *longue durée* again is worthy, but again, represents the exception rather than the rule. Compared to the foresight of the CPC's comprehensive developmental approach, the capitalist democracies of the EU member states remain preoccupied with short-term election cycle projects and are caught blindsided by crises such as the 2008 financial crash. GDPR can thus be seen as a warning, not a success story. It is symbolic of a greater sickness within the Western liberal order; that of the post-ideological turn in an age of neoliberal normativism, where legislation must undo past wrongs in order to build for the future. Its precepts guard only against perceived threat; again, emblematic of the crisis of capitalism that can no longer deliver sustainable futures for its citizens in a globalized world. The proof is in China's steadily rising living standards and falling corruption indices (Nederveen Pieterse, 2015) – the mirror image of Western decline. This does not forgive nor justify Chinese social repression and an autocratic political system in light of its ideological fortitude, but rather serves to deepen the debate around the morals and meaning of digital surveillance and its commercial applications that the contemporary world must address. Whilst China proceeds with constructive confidence, Europe lags behind, searching for a way to function in the global information civilization that is compatible with established Western political and social values.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Alaimo, C. & Kallinikos, J. (2017). Computing the everyday: Social media as data platforms. *The Information Society*, *33* (4), 175–191.

BBC News. (Producer). (2017, December 25). *China: The world's biggest camera surveillance network. BBC News* [Video].

Retrieved from https://www.youtube.com/watch?v=pNf4-d6fDoY
Bentham, J. (2009 [1791]). *Panopticon: Or the inspection house*. Whitefish, MT: Kessinger Publishing LLC.
Bray, D. (2005). *Social space and governance in urban China: The danwei system from origins to reform*. Stanford, CA: Stanford University Press.
Burgess, M. (2018, June 4). What is GDPR? The summary guide to GDPR compliance in the UK. *Wired*. Retrieved from http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislationcompliance-summary-fines-2018
Carr, N. G. (2011). *The shallows: What the internet is doing to our brains*. New York, NY: W. W. Norton & Company.
Chandler, D. (2015). A world without causation: Big data and the coming of age of posthumanism. *Millennium Journal of International Studies*, *43*(3), 833–851.
Christian, B. (2012). The A/B test: Inside the technology that's changing the rules of business. *Wired*. Retrieved from https://www.wired.com/2012/04/ff-abtesting/
China Internet Network Information Center (CNNIC). (2017, June). Statistical report on internet development in China. Retrieved from https://cnnic.com.cn/IDR/ReportDownloads/201706/P020170608523740585924.pdf
Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance & Society*, *15*(5), 609–625.
Cohen, J. E. (2016). The regulatory state in the information age. *Theoretical Inquiries in Law*, *17*(2), 369–414.
Cooper, L. (2016). Air pollution in China and IBM green initiatives [Blog post]. Retrieved from https://www.ibm.com/blogs/internet-of-things/air-pollution-green-initiatives/
Council of the European Union. (2015, June 11). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Retrieved from http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
Crouch, C. (2016). The march towards post? Democracy, ten years on. *The political quarterly*, *87*(1), 71–75.
Dai, X. (2018). Toward a reputation state: The Social Credit System Project of China. *SSRN*.
DLA Piper. (2019, February). DLA Piper GDPR Data Breach Survey: February 2019. Retrieved from https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey
Eaton, S. & Kostka, G. (2017). Central protectionism in China: The 'central SOE problem' in environmental governance. *The China Quarterly*, *231*, 685–704.
Economy, E. C. (2007). The great leap backward? The costs of China's environmental crisis. *Foreign Affairs*, *86*(5), 38–59.
European Data Protection Supervisor (EDPS). (2019). Annual Report 2018. Retrieved from https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf
European Union. (2016, May 4). EU General Data Protection Regulation (EU-GDPR). Retrieved from http://www.privacy-regulation.eu/en/
Ezrow, N., Frantz, E. & Kendall-Taylor, A. (2016). Institutions and development. In *Development and the state in the 21st century* (pp. 66–94). London: Palgrave Macmillan.
Global Times. (2017, June 14). Can big data help to resurrect the planned economy? Retrieved from http://www.globaltimes.cn/content/1051715.shtml
Halman, L. (1996, December). Individualism in individualized society? Results from the European values surveys. *International Journal of Comparative Sociology*, *37*(3–4), 195–214.
Harari, Y. N. (2016). *Homo deus: A brief history of tomorrow*. London: Jonathan Cape.
Harris, T. (2017). *How a handful of tech companies control billions of minds every day* [Video]. Retrieved from https://www.ted.com/talks/tristan_harris_the_manipulative_tricks_tech_companies_use_to_capture_your_attention

Harari, Y. N. (2018). *21 lessons for the 21st century*. London: Jonathan Cape.
Hawkins, A. (2017, May 24). Chinese citizens want the government to rank them. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2017/05/24/chinese-citizens-want-the-government-to-rank-them/
Heilmann, S. (2016, December). Leninism upgraded: Xi Jinping's authoritarian innovations. *China Economic Quarterly*, *20*(4), 15–22.
Hempel, J. (2018) What happened to Facebook's grand plan to wire the world? *Wired*. Retrieved from https://www.wired.com/story/what-happened-to-facebooks-grand-plan-to-wire-the-world/
Ho, P. (2009). Beyond development orthodoxy: Chinese lessons in pragmatism and institutional change. In Monique Kremer, Peter van Lieshout, & Robert Went (Eds), *Doing good or doing better: Development politics in a globalising world* (pp. 177–210). Amsterdam: Amsterdam University Press.
Hofstede, G. (1983). National cultures in four dimensions: A research-based theory of cultural differences among nations. *International Studies of Management & Organization*, *13*(1–2), 46–74.
Hvistendahl, M. (2017, December 14). Inside China's vast new experiment in social ranking. *Wired*. Retrieved from https://www.wired.com/story/age-of-social-credit/
Hvistendahl, M. (2018, March 14). A revered rocket scientist set in motion China's mass surveillance of its citizens. *Science*. Retrieved from http://www.sciencemag.org/news/2018/03/revered-rocket-scientist-set-motion-china-s-mass-surveillance-its-citizens
Jasanoff, S. (2005). Ordering knowledge, ordering society. In Sheila Jasanoff (Ed.), *States of knowledge: The co-production of science and social order* (pp. 13–45). London: Routledge.
Kaili, E. (2016, January 4). A new European vision founded on the values of Enlightenment and Humanism. *New Europe*. Retrieved from https://www.neweurope.eu/article/a-new-european-vision-founded-on-the-values-of-enlightenment-and-humanism/
Kaska, K., Beckvard, H. & Minárik, T. (2019). Huawei, 5G and China as a security threat. *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*. Retrieved from https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf
Kostka, G. (2018). China's social credit systems and public opinion: Explaining high levels of approval. *SSRN*. Retrieved from https://ssrn.com/abstract=3215138
Leonard, M. (2012). What does the new China think? In M. Leonard (Ed.), *China 3.0* (pp. 9–25). Retrieved from http://www.ecfr.eu/page/-/ECFR66_CHINA_30_final.pdf
Lee, K. F. (2018). *AI superpowers: China, Silicon Valley, and the new world order*. Boston, MA: Houghton Mifflin Harcourt.
Li, E. X. (2013). *A tale of two political systems* [Video]. Retrieved from https://www.ted.com/talks/eric_x_li_a_tale_of_two_political_systems
Lubman, S. (2017, December 5). The unprecedented reach of China's surveillance state. *China Policy Institute: Analysis*. Retrieved from https://cpianalysis.org/2017/12/05/the-unprecedented-reach-of-chinas-surveillance-state/
Lyon, D. (2003). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination* (pp. 13–30). London: Routledge.
Lyon, D. (2007). Surveillance, security and social sorting: Emerging research priorities. *International Criminal Justice Review*, *17*(3), 161–170.
Malgieri, G. & Comandé, G. (2017, November 1). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law*, *7*(4), 243–265.
Maurel, L. & Aufrère, L. (2018, May 25). GDPR: Online privacy is a collective issue! (A. Heathwood, Trans.). *SILex*. Retrieved from https://scinfolex.com/2018/05/25/gdpr-online-privacy-is-a-collective-issue/

Mayer-Schönberger, V. & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. London: Basic Books.
Meissner, M. (2017, May 24). China's Social Credit System: A big-data enabled approach to market regulation with broad implications for doing business in China. *MERICS China Monitor*. Retrieved from https://www.merics.org/sites/default/files/201709/China%20Monitor_39_SOCS_EN.pdf
Mitchell, A. & Diamond, L. (2018, February 2). China's surveillance state should scare everyone. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/
Nederveen Pieterse, J. (2015). China's contingencies and globalisation. *Third World Quarterly*, *36*(11), 1985–2001.
Nederveen Pieterse, J. (2018). Populism is a distraction. *New Global Studies*, *12*(3), 377–386.
Ness, S. & Chase, P. (2018, May 11) How GDPR could affect the transatlantic relationship. [Blog post]. Retrieved from http://www.gmfus.org/blog/2018/05/11/how-gdpr-could-affect-transatlantic-relationship
Newman, A. (2019, September 1). US and China are weaponising global trade networks. *Financial Times*. Retrieved from https://www.ft.com/content/a8ab8cd2-c99c-11e9-af46-b09e8bfe60c0
Pardes, A. (2018, May 24). What is GDPR and why should you care? *Wired*. Retrieved from https://www.wired.com/story/how-gdpr-affects-you/
Pendergast, T. (2018, March 28). The next Cold War is here, and it's all about data. *Wired*. Retrieved from https://www.wired.com/story/opinion-new-data-cold-war/
Polanyi, K. (2001[1944]). *The great transformation: The political and economic origins of our time*. Boston, MA: Beacon Press.
Rouvroy, A. (2012). The end(s) of critique: Data-behaviourism vs. due-process. In M. Hildebrandt & E. de Vries (Eds.), *Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology* (pp. 143–168). Abingdon: Routledge.
Ryz, L. & Grest, L. (2016). A new era in data protection. *Computer Fraud & Security*, *2016*(3), 18–20.
Sapio, F. (2017, December 11). The many facets of social credit. *China Policy Institute: Analysis*. Retrieved from https://cpianalysis.org/2017/12/11/the-many-facets-of-social-credit/
Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.
State Council. (2014). State Council notice concerning issuance of the planning outline for the construction of a social credit system (2014-2020) (Rogier Creemers, Trans). Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/
State Council. (2017). 国务院关于印发"十三五"市场监管规划的通知[现行有效]法宝引证码 [Notice of the State Council on Issuing the Plan for Market Regulation during the 13th Five-Year Plan Period]. Retrieved from http://lawinfochina.com/Display.aspx?lib=law&Cgid=289420
Stevis-Gridneff, M. (2019, September 10). EU's new digital czar: 'Most powerful regulator of big tech on the planet'. *The New York Times*. Retrieved from https://www.nytimes.com/2019/09/10/world/europe/margrethe-vestager-european-union-tech-regulation.html
Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5–8.
Vinocur, N. (2019). How one country blocks the world on data privacy. *Politico*. Retrieved from https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123
Wang, H., Mamingi, N., Laplante, B. & Dasgupta, S. (2003). Incomplete enforcement of pollution regulation: Bargaining power of Chinese factories. *Environmental and Resource Economics*, *24*(3), 245–262.

Woetzel, J., Seong, J., Wei Wang, K., Manyika, J., Chui, M. & Wong, W. (2017, August). China's digital economy: A leading global force. *McKinsey Global Institute*. Retrieved from https://www.mckinsey.com/global-themes/china/chinas-digital-economy-a-leading-global-force

Wu, T. (2010). *The master switch: The rise and fall of information empires*. New York, NY: Vintage.

Yim, M., Gomez, R. & Carter, M. (2017, January). Facebook's 'free basics' and implications for development: IT identity and social capital. *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 2590–2599). Washington, DC: IEEE Computer Society Press.

Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security, 2017*(6), 8–11.

Zhang, K. & Zhang, F. (2016). Report on the construction of the social credit system in China's Special Economic Zones. In Y. Tao & Y. Yuan (Eds.), *Annual Report on the Development of China's Special Economic Zones* (pp. 153–171). Singapore: Springer Singapore.

Zuboff, S. (2015). Big Other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

Brett Aho is a PhD student in the Department of Global Studies at the University of California, Santa Barbara. He has previously earned degrees from the University of Leipzig, University of Roskilde and the University of Redlands. His current research focuses on technology and regulatory governance in the United States, EU and China.

Roberta Duffield is a freelance researcher currently living in Cairo, Egypt. She holds previous degrees from the University of California, Santa Barbara and Oxford University. Her research focuses on urbanism, public space, and the politics of technology and infrastructure.