

Perng S. et al., Consuming disaster data: is IT ethical?, In: Boden, A., Jakobi, T., Stevens, G., Bala, C. Hgg., Verbraucherdatenschutz – Technik und Regulation zur Unterstützung des Individuums. Schriften der Verbraucherinformatik Band 1, 2021. DOI: 10.18418/978-3-96043-095-7\_06

# Consuming disaster data: is IT ethical?

Sung-Yueh Perng<sup>1</sup>, Monika Büscher<sup>2</sup>, Luke Moffat<sup>2</sup>

<sup>1</sup> Institute of Science, Technology and Society, National Yang Ming Chiao Tung University, Taiwan

<sup>2</sup> Centre for Mobilities Research, Department of Sociology, Lancaster University, UK.

*syperng@nycu.edu.tw; m.buscher@lancaster.ac.uk; l.moffat@lancaster.ac.uk*

**Abstract.** ‘Most people use disaster apps infrequently, primarily only in situations of turmoil, when they are physically or emotionally vulnerable. Personal data may be necessary to help them, data protections may be waived. In some circumstances, free movement and liberties may be curtailed for public protection, as was seen in the current COVID pandemic. Consuming and producing disaster data can deepen problems arising at the confluence of surveillance and disaster capitalism, where data has become a tool for solutionist instrumentarian power (Zuboff 2019, Klein 2008) and part of a destructive mode of one world worlding (Law 2015, Escobar 2020). The special use of disaster apps prompts us to ask what role consumer protection could play in safeguarding democratic liberties. Within this work, a set of current approaches are briefly reviewed and two case studies are presented of what we call appropriation or design against datafication. These combine document analysis and literature research with several months of online and field ethnographic observation. The first case study examines disaster app use in response to the 2010 Haiti earthquake, the second explores COVID Contact Tracing in Taiwan in 2020/21. Against this backdrop we ask, ‘how could and how should consumer protection respond to problems of surveillance disaster capitalism?’ Drawing on our work with the *is IT ethical? Exchange*, a co-designed community platform and knowledge exchange for disaster information sharing, and a *Societal Readiness Assessment Framework* that we are developing alongside it, we explore how co-design methodologies could help define answers.

# 1 Introduction

Mobile applications are a pervasive feature of the way goods and services are consumed, as well as how work and everyday lives are conducted. These online activities produce a ‘behavioural surplus’ that is highly valuable to corporations, governments, and other actors (Thrift 2011, Zuboff 2019, Crawford 2021). Its extraction has put ‘instrumentarian power’ into the hands of digital mega-corporations, a form of power that is fueled by categorisation and prediction that has made surveillance capitalism “as significant a threat to human nature in the twenty-first century as industrial capitalism was [and is] to the natural world”; it also poses “startling challenges to market democracy” (Zuboff 2019:v).

Disasters are similarly datafied, but shaped by complex and often contradictory processes. Data about disasters can be desirable for individuals affected by them as well as for those who attempt to organise a collective response. In her review of citizen mobile apps for disasters, Tan (2020) identifies 57 special disaster apps for disaster communications and response alongside general purpose communication platforms like Google, Facebook, Twitter, Weibo. These range from notifying apps like *ELERTS* to alerting and information apps like *Earthquake Alert!* to apps that collate situation reports (*GDACS Mobile*), support crowdsourcing (*Mobile4D*) and serve as platforms for collaborations (*Ushahidi*). COVID-19 has added a plethora of contact-tracing and health-monitoring apps with diverse levels of transparency (O’Neil 2020).

However, the surveillance, social sorting and manipulation this enables can be extraordinary. Phenomena like storms, floods, earthquakes, and pandemics disrupt normalcy and allow data controllers to make use of exceptions at a time when emergency response practitioners and victims increasingly depend on digital technologies. Many are physically vulnerable or in a state of heightened emotional tension. Highly personal data may be needed to help them, data protections may be waived and, in some circumstances, free movement and other liberties may be curtailed. Intensive data analytics and surveillance may be used for public protection, such as is occurring in the current COVID pandemic.

These measures may be appropriate in a crisis, but they can ‘mission creep’ and become normalized, eroding civil liberties and driving securitization. In other words, using disaster apps involves issues of, and beyond, consumer protection. Critical questions regarding the processes and consequences of datafying disasters should be asked. What ‘behavioral surplus’ is produced during disasters? Who benefits, who profits from it? What unintended consequences arise when surveillance capitalism (Zuboff 2019) meets disaster capitalism (Klein 2008)? When does the license to process disaster data begin and end?

In this paper we present a brief analysis of existing regulatory, policy and design responses and two case studies to better explore the potential role of consumer protection. What role could and should consumer protection organisations play in

safeguarding democratic liberties and values? Should consumer protection become citizen protection, or wider human protection for anyone touched by datafication, regardless of their legal status? Zuboff's call to reclaim human sovereignty, Amore's assertion that "algorithms are ethico-political beings in the world" (2020, p. 8) and Crawford's argument that we should stop talking about ethics and start talking about power (2021:2) inspire policy and design attempts to counteract problems of surveillant assemblages. At this juncture lies a unique opportunity to open up the debate for a more nuanced understanding of problems regarding surveillance and disaster capitalism. This debate extends to the development of co-design approaches *against* datafication and *for* data enfranchisement (in the sense of a liberation from data as a tool for instrumentarian power).

In the following, we first contextualise our analysis by examining key aspects of the confluence of surveillance and disaster capitalism (henceforth surveillance|disaster capitalism, Section 2) as well as their consequences. This then leads into a discussion of responses so far, exploring how researchers, regulators, consumers, and citizens have reacted and conceived how things might be otherwise. We argue that these current approaches focus on regulation, tactical resistance, and education. They are valuable, but insufficient. We paired our experience with societal readiness and ethical impact assessment with information garnered from case studies in order to develop recommendations that consumer organizations can use to press for change.

## 2 Solutionism, surveillance and inequality

Surveillance capitalism claims 'behavioural exhaust' for hidden commercial practices of extraction, prediction, and sales', to seek 'behavioural modification' or manipulation. It concentrates wealth among the 1%, whilst destroying nature and producing "a new instrumentarian power that presents startling challenges to market democracy...an expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty" (Zuboff 2019:v). Disaster capitalism intensifies these practices. The notion captures how long-established practices of profiteering from war and crises have become institutionalised strategies since 9/11. Klein (2008) argues that the 'shock doctrine' is "a political strategy of using large-scale crises to push through policies that systematically deepen inequality, enrich elites, and undercut everyone else." Surveillance|disaster capitalism enables data expropriation that promotes solutionism, exploitation of emotions, and a deepening of inequalities.

### 2.1 Solutionism

The burgeoning industry of digital health (Lupton 2013), the popularity of smart urbanism across the globe (Kitchin 2014), and the power of surveillance capitalism

mega-corporations (Zuboff 2019) indicate a deepening of solutionist (Morozov 2013) discourses, rationalities and practices. They recast complex health, urban and societal issues as problems that can be efficiently and economically solved by technological fixes in the forms of (big) data and data analytics, digital apps, and online platforms. The hope that data can rescue a world so deeply unsettled by COVID exemplifies that solutionist belief. The implementation of various digital technologies, from contact tracing to predictive artificial intelligence models of viral spread, have been posited as a ‘silver bullet’ solution to an inherently complex issue (Campbell-Verduyn 2021:4).

Contact tracing is the most common of the various data-centric ‘solutions’ and is currently being used in 158 countries<sup>1</sup>. By downloading the respective app and providing health and location data, people and governments had hoped that the technology would grant them health, freedom and safety. However, this viewpoint glosses over the high level of trust within a society and the sense of civic responsibility required for reaching a critical mass for the technology to be effective. It neglects the critical role of resistance from individuals and civil groups within society that can emerge when technology causes concerns, such as poorly designed privacy protection measures (Sandvig 2020). Furthermore, the focus on technological fixes prevents considerations of broader societal implications. For example, ‘smart home’ technology providers, as Maalsen and Dowling (2020) illustrate, can boast the use of biometric data for access control or the implementation of transaction functionalities for rent collection and eviction. But these technical solutions intensify surveillance at home, inappropriately justify data appropriation (health data for home access) and deepen social inequalities.

These are only some instances of the ‘data-centric techno-solutionist interventions’ mobilised amid the pandemic (see others in Leszczynski and Zook 2020). However, they demonstrate the immediate and harmful consequences that can be caused by a blind belief in data-centric solutionism as a means of disaster response. The unfolding of solutionism is inseparable from surveillance, the market and inequality, which we elaborate below.

## 2.2 Empathy

Disasters create anxiety and, thereby, new economic opportunities. In a survey, COVID researchers in Taiwan found that more than 40% of respondents experienced high levels of anxiety (Lu et al 2020). This ranged from worries about catching the virus to more generalised fears about the future. Climate change - the disaster that will shape humanity’s future - causes unprecedented levels of heightened anxiety, which is captured by new terms such as eco-anxiety or climate anxiety (Chen et al 2020). Young people are particularly vulnerable. One of the first national surveys showed that 25% of the Finnish population ‘recognized some

---

<sup>1</sup> <https://ourworldindata.org/grapher/covid-contact-tracing?tab=table>

form of climate anxiety in themselves’, and among ‘15- to 30-year olds, the percentage was over 33%’ (Panu 2020). This rise in anxiety amongst young people creates a problematic opportunity for surveillance|disaster capitalism. It has already prompted companies like Facebook to explore how they might profit from ‘moments when young people need a confidence boost’ (Reilly 2017), and there are strong incentives to seek out such moments in crises.

With new abilities to estimate “teen emotional states...based on how teens use the service, including “worthless,” “insecure,” “defeated,” “anxious,” “silly,” “useless,” “stupid,” “overwhelmed,” “stressed,” and “a failure”” (Reilly 2017), Facebook is able to identify vulnerability. Acute disaster situations, but also long-term recovery from disasters provide new opportunities for ‘empathetic’ capitalism. A worried person may be highly susceptible to promotions of health, insurance, ‘prepping’ or finance products, as well as ideological manipulation. But this turn to empathy is anything but empathetic (Pedwell 2012, Hunt 2018). In fact, it is the opposite, as people’s vulnerabilities are essentially being taken advantage of for profit. A new form of disaster capitalism is being enabled in this convergence with surveillance capitalism. As processing spills from everyday life into disastrous disruptions, behavioural surplus creates new and greater vulnerabilities to manipulate. The new economic order of surveillance capitalism is well set-up to claim even the most sensitive human experiences as free raw material - a form of accumulation by dispossession that is unequally performed.

### 2.3 Inequality

During the COVID-19 pandemic, many digital technologies have been introduced in the hopes of controlling the movements of viruses by regulating people’s movements through their data. Kaufmann and Audikana’s (2020) define ‘mobility capital’ as one’s ability to move, stay and equip themselves with relevant technologies. Included within their definition is the act of providing one’s movement data. This is unequally distributed among different societal members and can result in social exclusion. Similarly, Urry (2007) writes about ‘network capital’, where weak ties with acquaintances and friends of friends - vastly enlarged through social media - can often be just as important as deep personal relationships, because they “engender and sustain social relations with those people who are not necessarily proximate and which generates emotional, financial and practical benefit” (Urry 2007:197).

How much mobility and network capital one possesses has consequences on what economic and social life one can afford to live. As Urry argues, “social groups high in network capital enjoy significant advantages in making...social connections, the emotional, financial and practical benefits derived from what Bourdieu terms economic and cultural capital” (Urry 2007:197).

Hurricane Katrina laid bare the power of mobility and network capital in the way it dramatically altered people's lives. 'Middle class whites' were able to flee before the hurricane even made landfall, precisely because of their better access to transportation (higher car ownership) as well as their means of communication and established contacts elsewhere (Hartman and Squires 2006, see also Sheller 2016). The dynamics around mobility and network capital are different during pandemics, but the unequal consequences they engender are just as powerful. During COVID-19, being able to stay put and safe has often been available only to those in privileged social positions. Safety is acquired through accumulation of economic, social, cultural, mobility and network capitals. Access inequality to financial, technological, social, health and medical resources have been highlighted during the pandemic. Staying home is a realistic option only for those who have jobs that can be done at home that work for companies that offer the option of remote work. They would also require adequate access to the Internet as well as appropriate devices and apps. The increased use of technology that comes with home office also requires that one be digitally literate enough to operate these devices and apps (c.f. Milan, 2020). For some, these new work routines may have to be interlaced with everyday exercise or religious practices (Datta 2020).

Furthermore, if one has to move, the difference between risky and protected movements is also a product of unequal mobility and network capital. In order to have a safe journey, sufficient medical and healthcare resources (i.e. masks, sanitizer, vaccines), and technical means, like contact tracing apps, are needed to record one's whereabouts, state of health and contacts. Social and technical infrastructures need to include and protect those on the move.

However, for vulnerable social groups, these medical, social and infrastructural resources are often out of reach. For example, undocumented migrant workers in Singapore fall outside of the state apparatus that should count and include them into protective measures. These workers lack the means to take COVID tests and cannot use apps to show their health status, which means that they are absent from the datasets used to assess how different places are faring under the pandemic (Milan 2020). This lack of data about vulnerable groups, Pelizza (2020) argues, can further contribute to the production of pandemic alterity. As a result, narratives and misconceptions about the immunity or contagiousness of vulnerable social groups are created or sustained, furthering their status as 'the other'. Such groups include migrants, non-white ethnicities, (undocumented) workers or any combination of the above.

Digital technologies appropriated to combat COVID-19 have been closely linked to the development of smart cities and infrastructures in the past decade. There has been sustained critique, with many researchers revealing how inequalities are the results of such developments. For example, Willis (2019) demonstrated how India's Smart City Mission deprives 'the urban poor, street traders and those who live in informal settlements' of their rights to the city, while

Pilo (2021) discussed how smart metering can target socio-economically deprived groups as technological and political smart city projects exert gentrifying momentum. Everts (2020:261) observed a ‘dashboard epidemic’, where “pandemic dashboards are designed with suggestive curves and colour coding”, creating “matters of concern and direct[ing] attention and action in certain ways, foreclosing other paths”. He suggests that “pandemic dashboards hide as much as they reveal”. This is happening on a massive scale, as Datta (2020) highlighted, when she showed how almost half of India’s smart city Command and Control Centres were turned into ‘COVID-19 war rooms’ where monitoring and tracking of the movements of people and the virus takes place.

These aesthetically ‘smart’ Command and Control Centres and other smart city technologies are the materialisation of utopian urban imaginaries where visual narratives highlight technological wonders and sustain neoliberal values at the expense of the lives of the differently classed, gendered and racialised that are heavily impacted by these developments (Datta 2015, Wigley and Rose 2020). They enact a politics of visibility that hides the disadvantaged and disenfranchised, while creating a mirage of control. The actual control they provide is often very limited (Kitchin 2020) and smart city initiatives can be ‘placebo’ projects (Jirón et al 2021). Many smart city projects do little more than testify to a belief in technological fixes to complex issues. This in turn brings about damaging consequences, including the widening and intensifying socio-economic inequalities, neglect and obfuscation (e.g. invisibilisation, ways to game the system). Civic contestation, such as campaigns to highlight technological failures, are a poor match to the power of imaginaries of control.

Many examples discussed above are about the global South. Acknowledging the experiences and damaging consequences of smart solutionism in these places offers a perhaps surprisingly positive way forward. As Milan suggests, decolonial thinking, which draws on Atruro Escobar’s idea of ‘pluriverse’, can highlight the need to reject “uniformity, one-way solutionism, and the inability to think in terms of wider social relations, alterity and interdependence” (Milan 2020:5). To properly leverage data for disaster response strategies one must “think in terms of diversity and social relations, of flows and interdependence” and must also consider the consequences of differentiated distributions of mobility and network capital on the movements of people and data, “rather than border closures, oppressive social control, exclusionary datasets, or apps catering solely to the majority” (*ibid*). With this in mind, we now challenge the idea of an ‘inevitable’ trade-off of personal data for safety, convenience, and comfort.

### 3 No more trade-off: is it possible?

John Law (2015) describes how totalising imaginaries (like smart city solutionism) hold within them a specific ontology. He terms this the one-world world

(2015:132), a ‘Northern one-world metaphysics’ made by actors predominantly in the West since the 17th century. Their scientific and managerial practices morphed multiple realities into one reality by downgrading differences into mere perspectives. Feminist authors, like Lucy Suchman ([1987] 2007) and Donna Haraway (1991), have long argued that all knowledge is situated and partial. Arturo Escobar further developed these arguments with his ‘pluriversal politics’ to show that “the real, the possible, and the political are all joined at the hip” (2020:3) and how it is “because other possibles have been turned into “impossibles” that we find it so difficult to imagine other realities”. His suggestion that “another possible is possible” (*ibid.*) can prompt more ambitious innovation.

Digital technologies are not the cause of digitally driven one-world worlding or its destructive consequences. Zuboff shows how surveillance capitalism and its logics of accumulation by dispossession shape digital technologies to their aims and thereby drive a destruction of human nature. But there is nothing inevitable about this. In fact, digital technologies provide opportunities for ‘genuine participation’ and appropriation, they can support an ‘informational right to the city’ that has the potential to open up alternative digital social futures (Green 2006, Lefebvre 1991, Shaw and Graham 2017). A pluriversal focus on disaster allows us to bring different debates and responses to the destructive momentum of surveillance|disaster capitalism to join Zuboff’s call of “No more!” By doing so concrete alternatives can begin to be constructively articulated. This is not a straight path.

### 3.1 Moving beyond data trade-offs

The convenience, knowledge, and safety digital technologies present is said to ‘inevitably’ come at the cost of privacy and informational self-determination. However, Zuboff, argues, it is an act of dispossession; it is *deliberately made* inevitable. Firstly, by the fact that people are forced to give out personal data just to be able to participate in everyday life such as, for example, when they download apps – something now increasingly happening in regard to disaster information. People are unwittingly, or even unwillingly, complicit in this. Secondly, data dispossession happens by habituation. Because data collection is made as imperceptible as possible, people often do not notice when their data is being taken. This makes dissent and resistance very difficult. Some people do try to evade data collection, for example by turning their mobile phones off, by giving false data, or by deleting apps (e.g. the UK Covid App). There are also legal challenges, such as the 2021 lawsuit against Facebook for allegedly using photo face-tagging and other biometric data without the permission of its users<sup>2</sup>. But this only reveals a fourth power to dispossess, because if disaster capitalists “are pressured by public opinion

---

<sup>2</sup> <https://www.theguardian.com/technology/2021/feb/27/facebook-illinois-privacy-lawsuit-settlement>



or political pressure, they redirect by stonewalling, prevaricating, refusing to change, or tweaking the technology to avoid further controversy” (Soules 2020:212).

Discourses on the inevitability of trade-offs cement these powers. They are part of one-world worlding strategies in technology design and software engineering. Powerful critiques on surveillance studies have shown time and time again how wrong-footed these discourses are. For example, Introna (2007), revealed that denial is at the heart of this supposed inevitability – denial of the fundamental entanglement of the social and the technical. Trade-off discourse artificially separates ‘technical means’ from ‘social ends’ in order to make the logic of causal inevitability seem like common sense. Solove (2011) takes a legal perspective to show that inevitability is false, as there are many ways to balance privacy and security by “placing security programs under oversight, limiting future uses of personal data, and ensuring that programs are carried out in a balanced and controlled manner” (2011:207). Most recently, Kitchin (2020) highlighted how the discourse of trade-off is rooted in technological solutionism in the context of the COVID pandemic. Technological solutionism would mean public education, voluntary measures, and compliance could provide more effective means to support approaches where societies can have both privacy and public health.

Mayer-Schönberger cites the 2016 Trump elections and the Cambridge Analytica scandal to argue that digital “platforms have become weaponized to unravel not just privacy, but the very fabric of democracy” (2021:1). Zuboff goes even further and argues that it is “a threat to human nature”, because it “reduces us to our behavior” (2019:v, see also Ruppert et al 2013, on ‘doing subjects’). But digital disaster risk management holds other possibilities that contest the consequences of surveillance|disaster capitalism. We present two case studies.

### 3.2 Haiti and collaborative emergency response

At the time this work was written in August 2021, Haiti was reeling from a devastating earthquake and tropical storm Grace. A decade ago, in 2010, a similar disaster engendered the first ever mobilisation of “digital humanitarians” (Meier 2015). The 2010 Haiti Earthquake was a watershed for the emergent phenomenon of “crisis informatics” (Palen et al 2007). It changed disaster response. Self-organised mass-reporting and “online communication enabled a kind of [global] collective intelligence to emerge” (OCHA 2011), and thousands of volunteers converged online to aggregate, analyze, and map the flow of messages coming from Haiti. These volunteers were distributed across the globe, yet connected to Haiti in various ways, as victims, tourists, migrants, diaspora, friends, and relatives. Using Internet collaboration tools, they gathered and processed data, “wrote software, processed satellite imagery, built maps, and translated reports between the three languages of the operation” which included Haitian Creole, French, English

(*ibid*:27). Volunteers coordinated some of these efforts via digital crowdsourcing apps, including *OpenStreetMap* and *Ushahidi*. Over 4000 volunteers contributed to the Ushahidi Haiti Project (UHP) map, and their work provided valuable support to a number of in-the-field organisations, including the US Marines and the United Nations Disaster Assessment Search and Rescue teams (Morrow et al 2011). In many respects, the events within Haiti in 2010 could be seen as a participatory revolution for participatory “digital humanitarianism” (Meier 2015).

However, on closer inspection, one can see how the path is not straight. Meier’s story of digital humanitarianism is a form of one-world worlding in itself due to the many ambiguities suppressed by it. Firstly, while digital humanitarian efforts clearly made a difference, some professional responders called it a “shadow operation that was not part of the emergency response plan” (Morrow et al. 2011, 16). Secondly, there were inequalities. Mimi Sheller (2016) showed how the physical and digital influx of highly mobile international responders, from the World Bank to the voluntweeters with their birds-eye maps, coincided with a local population who mostly had neither the means nor the right to move outside the danger zone. Thirdly, many Haitians were unaware of the digital humanitarian response or did not have a voice in it (Clémento 2011). Fourth, even when data about need was registered on crowdsourced maps, it was not acted upon and, in effect, became part of a “communicative capitalism” where the expression and circulation of messages is not met by a commitment from those in power to listen, or engage (Dean 2009). As a result, the effort was in effect an exercise in “placating” rather than “genuine participation” (Green 2006). More recent examples show even more problematic practices of surveillance|disaster capitalism that prompt Sanfilippo et al (2020) to diagnose disaster privacy as a privacy disaster. One of their examples involves the US Federal Emergency Management Agency (FEMA), which released data about “2.3 million survivors of hurricanes’ Harvey, Irma, and Maria and the California wildfires in 2017 to a contractor” (*ibid*:1004).

But engagement in digital humanitarianism, crowdsourcing, collective intelligence, and crisis informatics does hold promise for a stronger, more collective, and more critically informed battle cry of “No more!” to surveillance|disaster capitalism. Since 2010, Haitian solidarity movements have coalesced online around demands for a #FreeHaiti and have also responded to the COVID pandemic and 2021 Haiti earthquake. These movements have formulated incisive analyses of the failures and disaster capitalism enacted by international disaster response organisations to the 2010 Earthquake, using hashtags like #2021isnot2010<sup>3</sup>. Part of this response is in resistance to “high tech, high visibility” projects that put profits for disaster capitalists over solidarity with the people affected by disasters.

---

<sup>3</sup> Sherwood, A. (2021) [Haiti: Why 2021 is and is not 2010](#). AlJazeera 13 Sep 2021

With such efforts, disaster risk management is pushed higher up the ‘ladder of participation’ (Arnstein 1969). Debates have shown that, all too often, concepts of participation (such as those, for example, in public health) translate into “patronizing attempts to “target” deprived communities with more education” (Green 2006:172) when there are real opportunities to take “citizens’ knowledge seriously” (Green 2006:173). One such example within public health was for vaccinations against COVID. Before we turn to our second case study, we would like to explore how experiences of digital humanitarianism and digital solidarity from Haiti resonate with responses to the problems of surveillance|disaster capitalism in consumer protection debates.

### 3.2.1 From digital literacy to data enfranchisement

What is it that hampers the development of opportunities to take multiple knowledges seriously? How do current consumer protection efforts address this? Inequity of privacy is a key factor:

Surveillance capitalists know everything *about us*, whereas their operations are designed to be unknowable *to us*. They accumulate vast domains of new knowledge *from us*, but not *for us*. They predict our futures for the sake of others’ gain, not ours (Zuboff 2019:11).

Many developers and designers within the field of technology are working on ways of supporting a greater sense of ownership and control over data for people. Consumer Informatics is a vibrant emergent field where these efforts are pushed. Stevens et al (2019) provided an overview of different consumer protection research perspectives and associated initiatives to develop digital literacy, consumer data sovereignty, as well as regulatory approaches. They call for a broader conception of the challenge as an assemblage of practices that come together to shape a *Lebenswelt* that enables surveillance capitalism. Pangrazio et al (2020) categorise efforts into regulatory, tactical resistance, and educational approaches designed to strengthen digital literacy. They explain in their work how data can be used for civic empowerment and argue that digital literacy is not simply about being able to make meaning from data. It is “heuristic to make sense of the relationship between functional symbolic codes and critical theories” like theories of surveillance|disaster capitalism (*ibid*:214).

But while Pangrazio et al argue that the “material “form” of data significantly influences how meaning can be made” (*ibid*:213), the researchers ultimately focused on pedagogies of giving more knowledge and tools to evade datafication. They focused on citizens as consumers rather than their wider human nature and subjectivity. They consider it to be a ‘cognitive matter’ when it is an embodied, material matter. Moreover, for most analysts, the option to simply not pursue certain innovations are not part of considerations. These omissions suggest a need to consider a wider process of data enfranchisement, precautionary principles and

material designs against datafication. These concepts will be further explored in the following section through the second case study.

### 3.3 Footprints for Democracy

Data has featured prominently over the course of Covid-19, and there have been many approaches and adaptations of contact tracing in many countries. Taiwan's ongoing adaptations, as we observed until May 2021, provide an opportunity to consider how processing data can be conducted in a way that addresses some of the problems of surveillance|disaster capitalism, even if only partially.

According to Taiwan's pandemic prevention protocols, the task of establishing contact histories, including footprints, has been the responsibility of public health agencies and doctors. During the pandemic, such data was collected by various means. The Ministry of Health and Welfare (MoHW) required business and transportation operators to keep a record of customers they served. The exact details required for these records changed over time. In the beginning, people were asked for the time/day of their visits, their real names, mobile or landline numbers, national identity numbers and/or contact address. This information was asked for when entering enclosed public places (e.g. shops, hospitals, government offices, schools if not students/pupils or staff, etc.) and when using public transportation or inter-city travel. These details were recorded by people writing them down on slips of paper provided by business operators, by filling in details using Google forms, or by staff entering the details onto the company's database themselves (database is a loose term here – each company might use different ways of recording).

The ways this data was provided, recorded and utilised raised significant privacy and surveillance concerns. It was unclear, at least initially, for how long the records would be kept by the operators, who exactly would have access to the records, how the data would be processed. There was a tendency to keep the records as long as possible in case relevant government agencies needed to access the records. On top of it all, any detail that people left on the paper could easily be seen by others. Furthermore, asking details such as one's national identity numbers were excessive for the purpose of contact tracing and could lead to identity theft.

The MoHW later published a guideline on the collection of personal information on the 22<sup>nd</sup> of May 2020. The guideline stipulated that the collection of personal information was to follow the principle of least intrusiveness, for example phone numbers. The same guideline also required that data should only be stored for 28 days. It was then to be destroyed with a record of the deletion kept on file. The data was only to be used by health agencies for the containment of the pandemic. Also, individuals were given the right to review, alter, delete or request a copy of the records held by the operators about them.

With the publication of the guideline, a regulatory framework was sketched to return data rights to the owners of said data in times of emergency. Although

appropriate processing of personal information is regulated by the Personal Data Protection Act and the Communicable Disease Control Act, these acts were not prepared for the intensified datafication of disasters as was seen during the pandemic. A simplified interpretation is that the Personal Data Protection Act is too generalised and cannot meet the demands of data use during emergencies. However, technologies of datafication outpaced the Communicable Disease Control Act rendering the act ineffective because many areas of datafication are unregulated. The guideline is therefore an important patch in the regulatory framework that prevents an excessive regime of datafication from further developing. It allows people to reclaim data ownership and rights and also sets out principles to govern future processing of personal data during this and other pandemics.

However, in May 2021, data collection for disaster response met new challenges. A sudden surge in community infection cases sent Taiwan into a Level 3 epidemic alert. Public anxiety rose as people feared unknowingly coming into contact with asymptomatic individuals. People were advised to make essential travels only (for food for example) and to work remotely. Despite the measures, the government was faced with growing numbers of cases, peaking up to 400-500 per day during the worst weeks. Although the numbers might not have been as high as in other countries, the Taiwanese government still faced the difficulty of tracing and establishing the chain of infection. These conditions made the previous data collection methods impractical – they were labour intensive, time consuming and stored by respective business operators. From a public health perspective, asking people to provide contact information right before entering a shop or an office also created a gathering of crowds furthering risks of infection.

An intensified scheme of data collection and analysis thus became desirable. More precise, detailed and continuous data could have potentially provided better knowledge about how people and viruses were moving and also show that the government was in control. But such data generation schemes rely on sophisticated digital technologies as well as smart infrastructure and could lead to conditions ideal for surveillance capitalism to take root, for ‘instrumentarian power’ to claim its legitimacy, and for marginal social groups to be left unprotected again.

Shortly after the alert, an alternative footprints data gathering mechanism was instead introduced. The government did not have to resort to a state-endorsed or platform-specific contacting app. While the alternative mechanism was implemented to enable large-scale data collection, it does not necessarily have to be accompanied by the shadows of datafying surveillance and its consequences.

At the core of the new mechanism are venue-specific QR codes that trigger mobile phones to initiate pre-formatted SMS messages which people have to send before accessing shops, offices or public transportation (an example is shown in Figure 1). The wording of the respective messages, translated by us, is as below:

Venue code: [code]. This SMS message is for the use of pandemic prevention only. [optional: number of additional people accompany the sender when entering the premises]

Before the official roll-out of the mechanism, each premise was required to apply for a venue code. They would then receive a QR code that is generated during the process of application. The QR code was then displayed on shop windows/doors, where people were required to scan it before entering. When they did so, the QR code triggered a pre-formatted SMS text where people could add additional information such as the number of people in the same trip. Sending the text records one's footprints, but only reveals essential information for monitoring movement: time, place, phone number of the sender and, if provided, the number of people in the trip.



Figure 1: Footprints SMS texts

Figure 2: Mixed footprints recording methods

Most importantly, paper-based data collection remains an option. Pictures of how they can be set up are shown above in Figure 2. This data collection method provides important alternatives for those experiencing difficulties. These difficulties included knowing how to tweak phone settings, affording and operating a mobile phone or accepting digital means of personal information collection. Other supplementary arrangements have also been made, such as providing rubber stamps with name and contact numbers to the elderly for recording footprints.

Once a text is sent, it is kept by the mobile phone operator. The MoHW does not have direct access to the database but, at the same time, mobile operators cannot extract location information from the data because only the MoHW has the key to link a code to a venue. This arrangement renders inappropriate use of the data more difficult. The data is retained for 28 days, after which time it is destroyed. If during this period a person became infected, the MoHW would obtain the mobile number of the individual and then ask relevant mobile operators to search for the timestamps and venue codes sent by the individual. The information would then be sent back to the MoHW to determine the times and places other people might have been infected. The MoHW would then provide a range of times and venue codes to mobile operators so they could identify the appropriate mobile phone users so they could be contacted. Mobile operators were also expected to send the phone numbers of these individuals back to the MoHW.

While social contact and physical movement are still turned into data through these mechanisms, they demonstrate how disaster data trade-offs are not inescapable. The scanning of QR codes or stamping contact details on paper make data collection material, felt and explicit, instead of running in the background without being noticed. The limitations placed on this kind of extensive data processing, such as the regulatory adjustments and indirect access to SMS data, stops data misuse. Moreover, the data collection methods with parallel footprints have the potential to materialise care for alterity and complex interdependency, such as people living in diverse socioeconomic conditions, those with differently-abled bodies and those who exercise different informational practices. The interweaving of regulatory, social, technological and material arrangements, like those seen in Taiwan's case, highlight the importance of people relating to data and disasters in embodied, material and pluriversal ways. This interweave also rejects the inevitability of trade-offs and allows for the exploration of practical alternatives.

## 4 Designing for appropriation and against datafication

As the cases above illustrate, people are appropriating digital technologies in ways that go beyond evading or resisting surveillance|disaster capitalism. These cases also demonstrate how it is possible to protect health and security without sacrificing privacy and civil liberties as 'inevitable' costs. However, supporting such efforts requires new ways of designing and using digital technologies. Below, we sketch two contributions to this effort.

### 4.1 Human Protection

It is, of course, important to recognize the importance of data sovereignty and informational self-determination towards better protecting consumer and citizen

rights. However, it should be noted that such protection needs to be broadened. Protective measures cannot become a right reserved for the privileged few. This protection would be much more accessible if it were to be self-organised and worked from the ground up in ways similar to the previous case studies (see also Tsing, 2015). This should be supported and augmented by institutional arrangements and remain open without limitations so that the health and data practices of the marginalized could also be included.

Expanding conceptions of consumer protection in this manner requires an alternative design approach that brings to life Lefebvre's (2003) vision of *autogestion* or self-management. Lefebvre envisions a better society, where the conditions of life are enabled by grassroots organisations and decentralised decision making instead of corporations (see also Purcell, 2014). In the context of an increasingly datafied society, this means exploring collaborative means of producing and processing data about consumption, disasters and more fundamentally social being and doing. It requires developing practices that pursue 'informational rights' (Shaw and Graham 2017), repudiate surveillance|disaster capitalism, traverse false dichotomies and solutionist fantasies. These practices would ultimately refuse to mobilise data in ways invited by the privileged few.

Designs that pursue informational rights and push against datafication require design practices that more actively explore pluriversal ways of living, relations between data and technology, as well as ways to devise and revise regulatory support. Technological fixes often presuppose, imply and even privilege a singular way of living and acting in the world. However, throughout this paper, we have demonstrated that disasters can be responded to with data in ways radically different from capitalist and solutionist visions. Specific ways of processing data implicate the lives of not only consumers and citizens but also others working and living alongside them without appropriate legal or institutional recognition (Pedroza 2019). Technical means of data processing alone is therefore not enough to push design development forward. Appropriate and effective associations with data within specific contexts of disaster response is also required. Furthermore, it is not enough to ask people to self-coordinate. Data processing protocols can become more effective if governments and regulations are re-arranged so as to accommodate or actively invite emergent forms of collaborative data processing. Types of collaborations, data capitalising and the way people relate to their data and digital technology are all prone to change. Even the disasters themselves, the many ways they can unfold, change unpredictably. Therefore, design against datafication has to go beyond establishing institutional arrangements. It must be open about data production and processing as well as its uses during analyses and in shaping decisions and actions to discover new challenges brought to people who are least protected.



## 4.2 Improving Design, making design reflexive: isITethical, SRL

isITethical? is an initiative led by a group of scholars in collaboration with the Public Safety Communications Europe Network that builds on completed and ongoing research, including research undertaken in a range of research projects. The “IsITethical? Exchange” combines an online resource (the “isITethical? Platform”) with creative ethical impact assessment. Professional development is facilitated by “Responsible Research and Innovation Advocates” (currently the founding members of the initiative), who use a mobile EtiKit to facilitate learning and build awareness of ethical, legal, and social issues. They also provide opportunities and have proactive responses. The kit comprises isITethical? information packs, a table-top game, a guide to the online platform, and ethical impact assessment workshop materials.

The isITethical? Exchange captures knowledge about existing and emerging ethical tensions and regulatory frameworks. It also consists of an open transnational knowledge base with information sharing in public safety and disaster responses. Its digital and material components and services facilitate broad-based dialogue and make knowledge actionable through examples of innovative pro-active practice, technological design, and regulatory responses. We seek to contribute to processes of standardisation and certification for products and services in public protection and disaster responses that adhere to ethical standards. The isITethical? Exchange is taking shape at <http://www.isitethical.org/>.

The isITethical Exchange is part of a broader effort to develop a framework for the Societal Readiness Assessment (SoRA), where societal readiness refers to the readiness of a socio-technical assemblage to be acceptable to, and good for, society. This framework is paired with an online learning platform that supports individuals, policy-makers, procurers, and communities in evaluating how well proposed ‘solutions’ support appropriation, utility, equity, and social good are criteria and Key Value Indicators serve assessment. Assessment includes scoring on a Societal Readiness Levels (SoRL) gauge. SoRA and SoRL can complement Technology Assessment and ‘Technology Readiness Levels’ (TRL). It is currently developed in the context of decarbonising transport, but the principles can be more widely applied. For example, a fully digitised, on-demand transport ‘solution’ may be highly practical and fit for appropriation by those who possess the mobile technologies needed. However, it may introduce socially unacceptable levels of surveillance and may be unavailable to the young, the old, the poor. As a result, it has low societal readiness. Its societal readiness can be improved by building privacy preserving techniques into its use of data and by involving citizens and stakeholders in an iterative design process that discloses and addresses unintended consequences through creative ethical and social impact assessment and design.

## 5 Conclusion

When Zuboff diagnoses an attack on human nature at the heart of surveillance capitalism, it is because through datafication, “the self is mobilised and activated in response to the calculation to which it is exposed” (Beer 2016, cited in Pangrazio et al 2020). This reduction of human nature and democratic enfranchisement to a “doing subject” (Ruppert et al 2013) is intensified through digital disaster apps and the confluence of surveillance and disaster capitalism. Our critical evaluation of these dynamics serves as a backdrop onto which we have presented avenues for new designs for appropriation. These designs would support meaning production and appropriation of disaster data through iterative developments, attention to societal values, and wide and effective implementation. The two case studies presented within this paper demonstrate that there can be ways of producing, processing and utilising disaster data that enable and encourage us to explore practical, infrastructural and institutional arrangements to resist surveillance|disaster capitalism. Tools like the isITethical Exchange and SoRA/SoRL can help the diverse actors involved in digital innovation recognise how people are situated in radically different social, economic, geopolitical and technological situations and how these differences manifest as diverging data practices. In addition, they can help anticipate unintended consequences and build levels of data literacy and informational self-determinations. They are key to broadening the scope of consumer protection to that of human protection. This manner of protecting human subjects in datafied worlds would do well to acknowledge that data is simultaneously informational, practical, embodied and material. Data requires design approaches that develop sensitivities and practices that enhance grassroots collaboration and involve institutional support.

## Acknowledgments

The research for this paper is supported by the Taiwanese Ministry of Science and Technology projects AI Cities in East Asia (MOST 109-2410-H-010-001-MY3) and the Research Center for Epidemic Prevention of the National Yang Ming Chiao Tung University (MOST109-2327-B-010-005). Support was also provided by the UK Engineering and Physical Sciences Research Council (EPSRC) DecarboN8 and the UKRI-GCRF project Gridding Equitable Urban Futures in Areas of Transition in Cali, Colombia and Havana, Cuba (GREAT) (grant numbers EP/S032002/1 and ES/T008008/1). This research was also supported in part by the UKRI Trustworthy Autonomous Systems project. We would like to thank the Public Safety Communications Europe Network for their insights and commitment to ethical innovation in our isITethical? Exchange collaborations as well as the organisers and participants in the Forum Verbraucherinformatik 2021 for their inspiration and comments on this paper.

## References

- Angulo, J. Fischer-Hübner, S. Wästlund, E. and Pulls, T. (2012): 'Towards usable privacy policy display and management', *Information Management & Computer Security*, vol. 20, no. 1, January 2012, pp. 4-17. <https://doi.org/10.1108/09685221211219155>.
- Arnstein, S. R. (1969): 'A ladder of citizen participation', *Journal of the American Institute of Planners*, vol. 35, no. 4, pp. (July): 216–224. -24.
- Campbell-Verduyn, M. (2021): *The Pandemic Techno-Solutionist Dilemma. Global Perspectives 2* (1). Pre-print
- Chen, S. Bagrodia, R. Pfeffer, C. C. Meli, L. and Bonanno, G. A. (2020): 'Anxiety and resilience in the face of natural disasters associated with climate change: A review and methodological critique', *Journal of Anxiety Disorders*, vol. 76, December 2020, pp. 1-16. <https://doi.org/10.1016/j.janxdis.2020.102297>.
- Clémento, J.-Y. (2011): *Ushahidi Project and Mission 4636 in Haiti: participation, representation and political economy. London School of Economics MA Thesis.*
- Crawford, K. (2021): *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.* New Haven and London: Yale University Press.
- Datta, A. (2015): 'New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city', *Dialogues in Human Geography*, vol. 5, no. 1, March 2015, pp. 3-22. <https://doi.org/10.1177/2043820614565748>.
- Datta, A. (2020): 'Self(ie)-governance: Technologies of intimate surveillance in India under COVID-19. *Dialogues in Human Geography*, vol. 10, no. 2, pp. 234–237. <https://doi.org/10.1177/2043820620929797>
- Escobar, A. (2020): *Pluriversal Politics The Real and the Possible*, Duke University Press, Durham, NC.. Berlin: DeGruyter
- Everts, J. (2020). *The dashboard pandemic. Dialogues in Human Geography* 10(2), 260-264.
- French, M. and Monahan, T. (2020): 'Dis-ease surveillance: How might surveillance studies address COVID-19?', *Surveillance & Society*, vol. 18 no. 1, March 2020, pp. 1-11. <https://doi.org/10.24908/ss.v18i1.13985>.
- Green, J. (2006): 'What role for critical public health?' *Critical Public Health*, September 2006; 16(3): 171–173.
- Hamm-Rodríguez, M. and Medina, C. L. (2021): 'Intra-caribbean solidarities and the language of social protest', *Applied Linguistics*, July 2021, pp.1-7. <https://doi.org/10.1093/applin/amab038>.
- Haraway, D. (1991): *Simians, Cyborgs, and Women: The Reinvention of Nature*, Routledge, New York and London.
- Hartman, C. and Squires G. D. (2006): *There is No Such Thing as A Natural Disaster: Race, Class, and Hurricane Katrina*, Routledge, New York.
- Hunt, R. (2018): *The Heart's Content: Media and Marketing after the Attention Economy*, MA Dissertation, Concordia University, Canada.
- Introna, L. (2007): 'Maintaining the reversibility of foldings: Making the ethics (politics) of information technology visible'. *Ethics and Information Technology*, vol. 9, no. 1, March 2007, pp. 11–25. <https://doi.org/10.1007/s10676-006-9133-z>
- Jirón, P. Imilán W. A. Lange C. and Mansilla, P. (2021): 'Placebo urban interventions: Observing smart city narratives in Santiago de Chile', *Urban Studies*, vol. 58, no. 3, August 2020, pp. 601-620. <https://doi.org/10.1177/0042098020943426>.
- Kaufmann, V. and Audikana, A. (2020): 'Mobility capital and motility', in O.E. Jensen et al (eds): *Handbook of Urban Mobilities*, Routledge, London and NY, 2020, pp. 41-47.
- Kitchin, R. (2014): 'The real-time city? Big data and smart urbanism', *GeoJournal*, vol. 79, no. 1, February 2014, pp. 1-14. <https://doi.org/10.1007/s10708-013-9516-8>.
- Kitchin, R. (2020): 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19', vol. 24, no. 3, January 2020, pp. 362-381. <https://doi.org/10.1080/13562576.2020.1770587>.
- Klein, N. (2008): *The Shock Doctrine: The Rise of Disaster Capitalism*, Penguin, London.

- Law, J. (2015): 'What's wrong with a one-world world?' *Distinktion: Scandinavian Journal of Social Theory*, vol. 16, no. 1, August 2015, pp. 126-139.  
<https://doi.org/10.1080/1600910X.2015.1020066>.
- Lefebvre H. (translated by Donald Nicholson-Smith) (1991): *The Production of Space*, Basil Blackwell, Oxford.
- Lefebvre H. (translated by Robert Bononno) (2003): *The Urban Revolution*, University of Minnesota Press, Minneapolis.
- Leonardi, P. M. (2020): 'COVID-19 and the new technologies of organizing: Digital exhaust, digital footprints, and artificial intelligence in the wake of remote work', *Journal of Management Studies*, vol. 58, no. 1, October 2020, pp. 249-253.  
<https://doi.org/10.1111/joms.12648>.
- Leszczynski, A. and Zook, M. (2020): 'Viral data', *Big Data & Society*, vol. 7, no. 2, November 2020, pp. 1-5. <https://doi.org/10.1177/2053951720971009>.
- Lu, W. H. Ko, N. Y. Chang, Y. P. Yen, C. F. and Wang, P. W. (2020): 'The coronavirus disease 2019 pandemic in Taiwan: An online survey on worry and anxiety and associated factors', *International Journal of Environmental Research and Public Health*, vol. 17, no. 21, October 2020, pp. 1-13. <https://doi.org/10.3390/ijerph17217974>.
- Lupton, D. (2013): 'Quantifying the body: Monitoring and measuring health in the age of mHealth technologies', *Critical Public Health*, vol. 23, no. 4, April 2013, pp. 393-403.  
<https://doi.org/10.1080/09581596.2013.794931>.
- Maalsen, S. and Dowling, R. (2020): 'Covid-19 and the accelerating smart home', *Big Data & Society*, vol. 7, no. 2, July 2020, pp. 1-5. <https://doi.org/10.1177/2053951720938073>.
- Mayer-Schönberger, V. (2021): 'Paradigm shift', *Computer Law & Security Review*, vol. 40, 1-3. <https://doi.org/10.1016/j.clsr.2020.105515>.
- Meier, P. (2015): *Digital Humanitarians. How Big Data Is Changing the Face of Humanitarian Response*. London: Routledge.
- Milan, S. (2020): 'Techno-solutionism and the standard human in the making of the COVID-19 pandemic', *Big Data & Society*, vol. 7, no. 2, October 2020, pp. 1-7.  
<https://doi.org/10.1177/2053951720966781>.
- Morozov, E. (2013): *To save everything, click here: The folly of technological solutionism*, PublicAffairs, New York.
- Morrow, N., Mock, N., Papendieck, A. and N. Kocmich. (2011): *Independent Evaluation of the Ushahidi Haiti Project Program*, no. 4. <https://reliefweb.int/report/haiti/independent-evaluation-ushahidi-haiti-project> [Accessed 20 September 2021]
- O'Neil, C. (2020, April 15): 'The COVID-19 Tracking App Won't Work'Neil. *Bloomberg Opinion*. <https://www.bloomberg.com/opinion/articles/2020-04-15/the-COVID-19-tracking-app-won-twork>
- OCHA. (2011). *Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies*. <https://reliefweb.int/report/world/disaster-relief-20-future-information-sharing-humanitarian-emergencies> [Accessed 20 September 2021]
- Palen, L., Vieweg, S., Sutton, J., Liu, S. B., Hughes, A. L., (2007): *Crisis informatics: Studying crisis in a networked world*. In: *Proceedings of the Third International Conference on E-Social Science*. Michigan, October 7-9, 2007.
- Pangrazio, L. and Sefton-Green, J. (2020): 'The social utility of 'data literacy'', *Learning, Media and Technology*, vol. 45, no. 2, April 2020, pp. 208-220.  
<https://doi.org/10.1080/17439884.2020.1707223>.
- Panu, P. (2020): 'Anxiety and the Ecological Crisis: An Analysis of Eco-Anxiety and Climate Anxiety', *Sustainability* 2020, vol. 12, 1-20 <https://doi.org/10.3390/su12197836>.
- Pedroza, L. (2019): *Citizenship Beyond Nationality: Immigrants' Right to Vote Across the World*, University of Pennsylvania Press, Philadelphia.
- Pedwell, C. (2012): *Economies of empathy: Obama, neoliberalism, and social justice*. *Environment and Planning D: Society and Space* 2012, vol. 30, pp. 280-297.
- Pelizza, A. (2020): "'No disease for the others": How COVID-19 data can enact new and old alterities', *Big Data & Society*, vol. 7, no. 2, July 2020, pp. 1-7.  
<https://doi.org/10.1177/2053951720942542>.

- Pilo, F. (2021): 'The smart grid as a security device: Electricity infrastructure and urban governance in Kingston and Rio de Janeiro', *Urban Studies*, January 2021, pp. 1-17. <https://doi.org/10.1177%2F0042098020985711>.
- Purcell, M. (2014): 'Possible worlds: Henri Lefebvre and the right to the city', *Journal of Urban Affairs*, vol. 36, no. 1, 2014, pp. 141-154. <https://doi.org/10.1111/juaf.12034>.
- Puschmann, C. and Powell, A. (2018) 'Turning words into consumer preferences: How sentiment analysis is framed in research and the news media', *Social Media + Society*, vol. 4, no. 3, September 2018, pp. 1-12. <https://doi.org/10.1177%2F2056305118797724>.
- Reilly, M. (2017): 'Is Facebook Targeting Ads at Sad Teens?', *MIT Technology Review*, 1 May 2017. <https://www.technologyreview.com/2017/05/01/105987/is-facebook-targeting-ads-at-sad-teens/>.
- Ruppert, E., Law, J. and Savage, M. (2013): 'Reassembling social science methods: The challenge of digital devices'. *Theory, Culture & Society*, vol. 30, no. 4, July 2013, pp. 22–46. <https://doi.org/10.1177/0263276413484941>
- Samuel, G. Roberts, S. L. Fiske, A. Lucivero, F. McLennan, S. Phillips, A. Hayes, S. and Johnson, S. B. (2021): 'COVID-19 contact tracing apps: UK public perceptions', *Critical Public Health*, April 2021, pp. 1-13. <https://doi.org/10.1080/09581596.2021.1909707>.
- Sandvik, K. B. (2020): "'Smittestopp": If you want your freedom back, download now', *Big Data & Society*, vol. 7, no. 2, July 2020, pp. 1-11. <https://doi.org/10.1177/2053951720939985>.
- Sanfilippo, M. R. Shvartzshnaider, Y. Reyes, I. Nissenbaum, H. and Egelman, S. (2020): 'Disaster privacy/privacy disaster', *Journal of the Association of Information Science Technology*, vol. 71, no. 9, September 2020, pp. 1002-1014. <https://doi.org/10.1002/asi.24353>.
- Shaw, J. and Graham, M. (2017): 'An informational right to the city? Code, content, control, and the urbanization of information', *Antipode*, vol. 49, no. 4, September 2017, pp. 907-927. <https://doi.org/10.1111/anti.12312>.
- Sheller, M. (2016): 'Connected mobility in a disconnected world: Contested infrastructure in postdisaster contexts', *Annals of the American Association of Geographers*, vol. 106, no. 2, January 2016, pp. 330-339. <https://doi.org/10.1080/00045608.2015.1113114>.
- Sherwood, A. (2021): 'Haiti: Why 2021 is and is not 2010', *Aljazeera*, 13 September 2021. <https://www.aljazeera.com/opinions/2021/9/13/haiti-why-2021-is-and-is-not-2010>.
- Solove, D.J. (2011): *Nothing to hide. The false tradeoff between privacy and security*. New Haven and London: Yale University Press.
- Soules, M. (2020): 'Surveillance capitalism pandemic', *New Explorations. Studies in Culture & Communication*, vol. 2 (Autumn 2020), pp. 201-220.
- Stevens, G., Boden, A., Winterberg, L., Gómez, J. and Bala, C. (2019): 'Digitaler Konsum: Herausforderungen und Chancen der Verbraucherinformatik'. *Wirtschaftsinformatik 2019 Proceedings*, February <https://aisel.aisnet.org/wi2019/workshops/papers/6>. [Accessed 20 September 2021]
- Suchman, L. ([1987] 2007): *Human-machine Reconfigurations: Plans and Situated Actions* (Vol. 2nd). Cambridge University Press, Cambridge.
- Tan, M. L. (2020): *Usability of disaster apps: Understanding the perspectives of the public as end users*, PhD Thesis, Massey University, New Zealand. <http://hdl.handle.net/10179/15393>.
- Thrift, N. (2011): 'Lifeworld Inc—And what to do about it', *Environment and Planning D: Society and Space*, vol. 29, no. 1, February 2011, pp. 5–26. <https://doi.org/10.1068/d0310>
- Tsing, A. L. (2015): *The Mushroom at the End of the World: On the Possibility of Life in Capitalist Ruins*, Princeton University Press, Princeton, NJ.
- Urry, J. (2007): *Mobilities*, Polity, Cambridge.
- Wigley, E. and Rose, G. (2020): 'Who's behind the wheel? Visioning the future users and urban contexts of connected and autonomous vehicle technologies', *Geografiska Annaler: Series B, Human Geography*, vol. 102, no. 2, April 2020, pp. 155-171. <https://doi.org/10.1080/04353684.2020.1747943>.
- Willis, K. S. (2019). 'Whose Right to the Smart City?', in P. Cardullo, C. D. Felicianantonio, and R. Kitchin (eds): *The Right to the Smart City*. Emerald Publishing, Bingley, June 2019, pp. 27-41. <https://doi.org/10.1108/978-1-78769-139-120191002>.

Zuboff, S. (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books, London.