Ethics and Information Technology (2023) 25:60
https://doi.org/10.1007/s10676-023-09732-8

ORIGINAL PAPER

Public health measures and the rise of incidental surveillance: Considerations about private informational power and accountability

B. A. Kamphorst[1] · **A. Henschke**[2]

Accepted: 18 October 2023 / Published online: 16 November 2023

Abstract

The public health measures implemented in response to the COVID-19 pandemic have resulted in a substantially increased shared reliance on private infrastructure and digital services in areas such as healthcare, education, retail, and the workplace. This development has (i) granted a number of private actors significant (informational) power, and (ii) given rise to a range of digital surveillance practices incidental to the pandemic itself. In this paper, we reflect on these secondary consequences of the pandemic and observe that, even though collateral data disclosure and additional activity monitoring appears to have been generally socially accepted as inevitable consequences of the pandemic, part and parcel of a larger conglomeration of emergency compromises, these increased surveillance practices were not directly justified by appeals to solidarity and public health in the same way that the instigating public health measures were. Based on this observation, and given the increased reliance on private actors for maintaining the digital space, we argue that governments have a duty to (i) seek and ensure that there are justifications for collateral data disclosure and activity monitoring by private actors in the context of (future) public health emergencies like the COVID-19 pandemic, and (ii) regulate and provide accountability mechanisms for and oversight over these private surveillance practices on par with governmental essential services that engage in surveillance activities.

Keywords Surveillance · Justification · Accountability · Oversight · Public health · Pandemic response

Introduction

From the beginning of the COVID-19 pandemic, worries about surveillance were at the forefront of public debate about governmental responses to the pandemic. In response to public health measures such as the use of aggregated mobile phone location data (Grantz et al., 2020), the deployment of GPS-based home quarantine monitoring apps (e.g., Poland's Kwarantanna Domowa app), and the introduction of proximity trackers (e.g., the Dutch "CoronaMelder" App), there has been significant and continuous social and political resistance that, at least in Western countries, forced governments to become explicit about the justification for these instruments and to regulate their legitimate and proportional use (cf. Blasimme et al., 2021). But with the public eye focused on the public health measures themselves, and on the direct consequences of *governmental* surveillance for people's liberty and privacy, another development received less attention, namely the way in which various lockdown and home confinement measures significantly increased our shared reliance on private infrastructure and digital services in areas such as healthcare, education, retail, leisure, and the workplace. Moreover, there has been little public discussion of the implications of this shift to private services in terms of accountability and governance.

After laying out our terms ("Section I: Terms and concepts"), we will proceed to show that the public health measures for mitigating the COVID-19 pandemic increased the incidental surveillance of various "day-to-day" activities by these private actors ("Section II: The rise of incidental surveillance"), and thereby granted significant informational power to a select number of private actors ("Section III: Considerations about justifications and private power"). As a preliminary example, consider how the requirement to work

✉ B. A. Kamphorst
bart.kamphorst@wur.nl

A. Henschke
a.henschke@utwente.nl

[1] Department of Social Sciences, Wageningen University, Wageningen, The Netherlands

[2] Philosophy Section, Faculty of Behavioural, Management and Social Sciences, University of Twente, Twente, The Netherlands

from home has not only allowed tech giants to collect more data about logins and application usage but has also given employers more insights into workplace behaviour. To firmly establish this point, we will survey a range of examples of incidental surveillance practices in different domains.

Though this additional surveillance appears to have been generally socially accepted as an inevitable consequence of the pandemic, part and parcel of a larger conglomeration of emergency compromises, we contend that these practices may have lacked justification, as they were not directly justified by the same appeals to solidarity and public health used for justifying the instigating public health measures themselves. In light of this observation, we will argue in the final Section of the paper ("Section IV: The need for accountability and oversight") that governments who enforce lockdown and work-from-home public health measures have a duty to determine how and to what extent collateral data disclosure and activity monitoring by private actors can, in fact, be justified—both in relation to the recent pandemic and in contexts of future public health emergencies. Moreover, given the enduring, increased reliance on private actors for maintaining the digital space, we will argue that these actors are de facto providing an essential service, and should therefore have their surveillance practices be regulated and be subject to accountability mechanisms and oversight on par with governmental essential services that engage in surveillance activities.

Section I: Terms and concepts

In this section, we will clarify how we are using particular terms. Note that we are not seeking to offer comprehensive or final definitions for the concepts denoted by these terms, but rather to establish the conceptual boundaries around the terms such that our use of them in the paper can be understood. In what follows, we offer descriptions of our use of 'incidental surveillance', 'informational power', and 'accountability'.

As we will argue in "Section II: The rise of incidental surveillance", the COVID-19 pandemic has brought about a range of different surveillance practices. We follow David Lyon's description of surveillance in which the term denotes the "focused and purposive attention to objects, data, or persons" (Lyon, 2009). There are many instances and examples of how surveillance technologies and practices were used to monitor and arrest the spread of COVID-19, be it by public actors (e.g., public hospitals collecting COVID-19-related hospital admission data to support incident management), private actors (e.g., corporations offering COVID-19 tracking apps), or a via public–private partnerships (e.g., governments collecting mobility data through telecom providers).[1] These surveillance practices (and the underlying delegation structures) raise important questions of their own, including whether the collected data can be used for other purposes (including research and for-profit purposes) than they were originally collected for ("mission creep"; see, e.g., Pagliari, 2020; Gerlitz & Häring, 2023). However, those questions are not what we are concerned with here.

Instead, the focus of this paper is on 'incidental surveillance'. By incidental surveillance we mean surveillance whose practices shifted because of the COVID-19 pandemic but were not concerned with a focused and purposive attention to COVID-19 itself. For instance, consider that, due to people working from home, the capacity for workplace surveillance increased. This surveillance was *incidental* to pandemic-related public health measures such as lockdowns, in the sense that the corporations facilitating remote "teleworking" were not tasked with collecting COVID-19-related data, and yet increased their surveillance as a result of the COVID-19-related public health measures. Incidental is significant here, as the surveillance practices that we are concerned with in this paper are incidental to the public health response to COVID-19. As we will argue, this creates a unique challenge in that the justifications for the public health measures themselves, including those for direct COVID-19 surveillance, do not necessarily transfer over to the incidental surveillance.

The second term to introduce is that of 'informational power'. Here, we recognise that 'power' is itself a contested term. As Joseph Nye Jr. puts it, "[n]o one definition is accepted by all who use the word, and people's choice of definition represents their interests and values" (Nye, 2011, p. 5). It is the subject of a debate that we cannot attempt to settle here.[2] However, we can give some background and explicate how we are using the term. Power can be understood in quite a general sense, where it "means the capacity to do things" (Nye, 2004, p.1). However, it is not just about getting things done but also about "the ability to influence behaviour of others to get the outcomes one wants", be it through coercion, or inducement, or even by simply offering an attractive option (Nye, 2004, p. 2). Nye also recognises that power can be understood in two further ways. Policy makers, for instance, "frequently define power simply in terms of the resources that can produce outcomes" (Nye, 2011, p. 8). In contrast, "[b]ehavioral definitions judge

[1] For a broad overview of the ethical and political challenges with surveillance in times of emergency, see Macnish and Henschke (forthcoming).

[2] Steven Lukes, for instance, defined power as a situation in which "A exercises power over B when A affects B in a manner contrary to B's interests" (Lukes, quoted in Macdonald, 1976), while K. I. Macdonald criticises the centrality that interests play in Lukes' account (Macdonald, 1976).

power by the outcomes that are determined after the action ["ex post"] rather than before ("ex ante")" (Nye, 2011, p. 4). So we may understand power as resources or as outcomes.

In understanding *informational* power, then, we want to recognise both control over informational resources, and the ways in which that information can bring about particular outcomes. For instance, sharing or withholding one's vaccination status is a form of informational power. Likewise, using one's vaccination status to alter behaviour and thus outcomes is also informational power. Combining these two elements of power, informational power can thus be understood as the capacity to use, share, withhold, or manipulate information (as a resource) in order to bring about or prevent some outcome in the world.

For our purposes, this notion of informational power is not only relevant to the way information may be used by individuals to influence their own behaviour and that of others, but also more generally to the control over information that governments and corporations have.[3] If a governmental department has a database about COVID-19 infections in the community, and they control who can access that information, they have informational power. Likewise, if a private testing facility uses the results of analysis of COVID-19 infection patterns to offer advice to their government on COVID-19 policies, then they have informational power as well. Given the value that information now has in society, informational control can also confer social, political, economic, and legal power on those who have that control. In "Section III: Considerations about justifications and private power", we discuss the implications of increased informational power arising from incidental surveillance.

The final concept we want to address here is accountability. In particular, we want to draw out the difference between accountability and oversight. Oversight is a process in which an overseer has access to, or some awareness of, the actions, decisions, or behaviours of some target of attention. In the context of governance, oversight is typically thought of as the review and evaluation of selected activities by governmental agencies.[4] In contrast, what is central to accountability of public actors is that it is "*a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor may face consequences*" (author's original emphasis, Bovens, 2007, p. 450). The relevant point here is that accountability involves some justification or explanation of actions, decisions, or behaviours, to a forum, with the relevant actor perhaps facing some consequence for their conduct. It is "the obligation to explain and justify conduct, [which] implies a relationship between an actor, the accountor, and a forum, the accountholder or accountee" (Bovens, 2007, p. 450). Accountability requires interaction between the actor and some others, viz. with those others having some power as a result of their position. As we will see, the notion of accountability as the need to offer a justification, coupled with changes in informational power, is crucial in relation to incidental surveillance.

Section II: The rise of incidental surveillance

In this section, we outline a wide set of areas in which the COVID-19 pandemic led to a rise in incidental surveillance. The first and very prominent domain is healthcare. Due to the increased strain on hospitals, combined with limitations imposed on people's physical movement by lockdown measures, many healthcare services entered into collaborations with private companies to offer online consultations (Mann et al., 2020; Richardson et al., 2020), remote health monitoring of health biomarkers such as blood pressure, blood glucose levels, and heart rate (for review, see Lukas et al, 2020), and develop automated health monitoring and treatment apps (Gerli et al., 2021; McGreevey et al., 2020; Parviainen & Rantala, 2022). To an extent, this process of digitalization was already ongoing, but the pandemic acted as a catalyst for change in this regard (Shah & Schulman, 2021; Bloem et al., 2020; Lau et al., 2020). In Germany, for example, the largest doctor-patient portal "Jameda" reported explosive growth of the demand for their video consultation software at the start of the pandemic (Jameda, 2020). Likewise, the Barcelona-based start-up "Mediquo" reported significant increases in demand (ConSalud, 2020). Elsewhere, healthcare professionals took to popular commercial communication platforms such as Zoom, Microsoft Teams, and WhatsApp to offer online video consultations (Vargo et al., 2021), despite the known drawbacks of such platforms in relation to the protection of health data (Masoni & Guelfi, 2020).

As a result, increasingly large volumes of health-related data began to flow to private actors, increasing their surveillance and their informational power by allowing them to gain more insights into people's health status as well as health-related preferences and behaviours. Depending on the type of platform, these insights may be inferred from actual health measurements (e.g., cardiovascular data from a home ECG monitor) or from mining access and event logs, from which plenty of commercially interesting information (e.g., for targeted advertisements) can already be gleaned (e.g., how frequently people interact with healthcare providers, whether they do so during business hours or in the evening,

[3] A point recognized also by Daniel J. Solove when he wrote that data mining creates power imbalances and that "[d]ata mining allows executive officials and agencies relatively insulated from public accountability to exercise significant power over citizens." (Solove, 2008, p. 194).

[4] For an overview of the legal literature on oversight, see Ogul and Rockman (1990).

what type of healthcare they seek, whether they prefer a particular practitioner, etc.).

The transitions to remote healthcare solutions were responses to an urgent practical problem—namely how to continue offering adequate and appropriate healthcare to those in need during a public health emergency. It is therefore worth noting that our aim here is not to deny the effectiveness of these responses, nor to find fault with the motivation of the healthcare professionals or the willingness of patients to consent (which may be especially understandable if they felt there was no acceptable alternative; cf. Kamphorst et al., 2023). Rather, the aim is to draw attention to the phenomenon of incidental surveillance and, on a general level, to question the extent to which increased surveillance by private actors stemming from this shift to digital, remote healthcare solutions is justified.

Importantly for this paper, the justifications for such surveillance differ from that of direct COVID-19 surveillance. In the former, the justifications are the need to provide access to essential clinical healthcare services. In the latter, the justifications are public health justifications explicitly linked to the need to monitor and ultimately mitigate the effects of the COVID-19 pandemic. This distinction between clinical medicine and public health is important as the two practices ultimately have different moral mechanics (O'Neill, 2004). We also note that the ethical justifications for clinical healthcare differ from the ethical justifications for public health. Clinical healthcare is primarily concerned with the rights of the individual patient, and the responsibilities that particular medical professionals have towards that individual. In contrast, public health ethics is more concerned with healthcare at a population level, with the professional responsibilities being directed towards the collective. "While medicine focuses on providing treatment and care for individuals as patients, public health focuses on preventing disease and disability for the greater population. Medicine involves a relationship between a physician and an individual as a patient. Public health involves relationships between members in the community, various professionals and the government" (Latheef, forthcoming). Clinical healthcare justifications will draw from moral value of the individual whereas public healthcare justifications will draw from the moral value of the population. Thus, given the different surveillance practices being discussed—clinical and public health—it must be ensured that both sets of surveillance practice are justifiable in general, and justified in the particular cases.[5]

Shifting from the contexts of clinical and public healthcare, let us examine more domains where incidental surveillance increased because of the pandemic and the associated public health measures, beginning with the workplace. As the first lockdowns were implemented at the beginning of the pandemic, working from home became the norm for many "nonessential" workers around the world (e.g., Ipsen et al., 2021). For many, being able to work from home was–and frequently still is–facilitated by large-scale digital online platforms such as Zoom, Microsoft Teams and Office 365, Google Docs, Calendar and Meet, and various Virtual Private Network (VPN) solutions to access company documents.[6] This increase in the use of VPN services and cloud-based applications effectively resulted in people leaving an increasingly large digital footprint that details how they spend their work days.

Though these platforms existed before the pandemic, the scale at which they became used was unprecedented.[7] As such, the private actors running these platforms gained access to more behavioural data than ever before, which they could mine and use for commercial purposes. One way in which the collected data was commercialized was by selling it back to the organizations themselves. Office 365, for example, offered its pro-tier customers "usage analytics" to gain insights into how their organization is using the various services, which include individual user activity reports (Microsoft, 2022). As such, employers were given extensive tools of surveillance for checking on their employees. Workplace examples clearly demonstrate the rise of incidental surveillance.

Another consequence of the explosive use of video conferencing in the workplace was the normalization of making and sharing video content. Many professional meetings, including job interviews and assessments, started being recorded, often explicitly through the video conferencing software, but potentially also illicitly by participants making use of third-party software or smartphones to make screenshots and screen recordings. These recordings are then typically stored, not only on local devices and hard drives, but also in cloud-based storage, where they are possibly retained in perpetuity. And while these recordings may have legitimate uses, such as sharing past seminars with new colleagues, or re-watching meetings to extract action points, they also pose serious risks, as people cannot fully control what happens with the information they (inadvertently) shared (cf. Kamphorst & O'Neill, in prep.). As O'Neill has phrased it, digital recordings can be thought of as "digital wormholes," with snippets and fragments of one's past self

[5] For more on the distinctions between clinical and public health care and surveillance, see Latheef (forthcoming). On pandemic surveillance needing to be both justifiable in general, and justified in specific cases, see Henschke (forthcoming).

[6] Notably, this development has also led to an increase in successful cyber-attacks (Borkovich & Skovira, 2020).

[7] In 2019, Microsoft Teams had an estimated 20 million users, which had grown to 250 million by July 2021 (Curry, 2022).

showing up at unexpected times and in unexpected contexts (O'Neill, 2021).[8] Moreover, as we will discuss, the justifications offered for such surveillance are clearly different from any public health justifications related directly to COVID-19.[9]

The worries about recordings also carry over to the domain of education. During the pandemic, online lectures by teachers and professors were often recorded, at times without permission. Students, too, partook in recorded seminars, and were frequently asked to prepare and submit video content to online assignment platforms. But perhaps the most noteworthy form of surveillance in this domain was the automated proctoring of exams (e.g., Kharbat & Abu Daabes, 2021). With automated proctoring software, university students were required to turn on their webcams, do a full scan of their surroundings—oftentimes including their personal belongings—and then make the exam while allowing a black-box algorithm from a private company to analyse the live video stream to detect suspicious behaviour (Coghlan et al., 2021). This controversial practice caused public criticism, with students in various countries making complaints, starting petitions, and even taking universities to court (Rechtbank Amsterdam, 2020).

Much remains to be said about the practice of online proctoring, but since it took shape in response to the significant challenge of ensuring academic continuity during lockdown, and its legitimacy has so far been upheld, we will not concern ourselves here with the (un)desirability of this particular kind of surveillance. Rather, our more modest aim is to consider this type of additional tracking and oversight as fitting a larger pattern of surveillance expansion that, on the whole, requires a particular set of justifications that are distinct from the justifications directly related to COVID-19 public health measures.

To complete the picture of incidental surveillance, let us consider the domains of online home entertainment and retail. Like the tech giants facilitating remote communication, large online media platforms such as Netflix, Disney+, Hulu, Amazon Prime and Apple TV, as well as major gaming platforms like Microsoft, Nintendo and Sony, reported tremendous growth in their subscriptions and sales as a result of lockdown and curfew measures.[10] With theatres, bars, restaurants, clubs, and gyms all closed, people "en masse" turned to on-demand video and gaming platforms as alternative forms of entertainment. Consequently, these platforms all saw huge peaks in the numbers of individuals whose viewing and usage behaviour and media preferences they could now track. Parallel to the rise in use, with unemployment high in various sectors and working from home the new normal, interactions (and therefore surveillance) were not restricted to "after hours". As a result, these companies could build user profiles that not only detailed which kinds of content people like, but also when they take their lunch breaks, take time off from work, take care of their kids, and so on. Thus, the capacity for entertainment providers to engage in incidental surveillance significantly increased.

Finally, the lockdown and social distancing measures accelerated the transformation of the retail landscape. With people unable to go out, many "nonessential" businesses with physical stores, including restaurants, saw themselves forced to further develop their digital presence by opening web shops, and consumers were quick to get on board. Established online retailers such as Amazon, Walmart, and Zalando benefited tremendously from the lockdowns.[11] And though "essential" stores such as supermarkets, pharmacies, and drugstores mostly remained open, they too saw a substantial increase in their online sales (cf. Tyrväinen & Karjaluoto, 2022). In effect, this meant that an increased number of consumers started sharing more and more information about their consumer preferences and spending habits with more parties and with an increased frequency. And since these online transactions were processed by payment gateways such as PayPal or Stripe, and online orders were subsequently delivered by parcel delivery companies such as DHL, UPS, DPD and FedEx, they too gain insights into consumer behaviour (e.g., who orders from what stores, with what frequency, etc.).

The picture that emerges from the surveyed domains shows that incidental surveillance by private actors has become ubiquitous and is likely to stay that way for the foreseeable future. Before moving to a discussion of the implications of this development, there are three further remarks we would like to make. First, the breadth of the domains we surveyed shows just how pervasive the phenomenon really is.

[8] The most obvious risk in this category is that recordings end up making headlines in popular media, which happened for instance with journalists and politicians who accidentally exposed themselves on camera, or with the plastic surgeon who appeared in a Zoom court meeting while operating on a patient (see Fazio, 2021). Another real but less obvious risk is that people's video content will be used to train machine learning algorithms to create "deep fake" videos (cf. Masood et al., 2022).

[9] For more on the ethics of workplace surveillance, see Miller & Weckert, 2000.

[10] For numbers about video content subscriptions, see Sweney (2020). For the gaming industry, consider that Sony almost doubled the sales of Playstation 4 games in the second quarter of 2020 (Yeung, 2020), and sales for the Nintendo Switch even tripled that year (Espiner, 2020).

[11] For example, in 2021, Amazon's profits had increased by 200% compared to what they were before the pandemic (Weise, 2021). We note that these levels of profits were not sustained, and Amazon and others started cutting workers from mid 2022 onwards. However, the points about significant increases remain.

At the same time, it should be emphasized that the domain contexts have different characteristics.[12] As scholars such as Nissenbaum (2009) and O'Neill (2022) have argued, different contexts may have different ends or purposes, which will co-determine by which standards to evaluate certain techno-social changes in those contexts. For example, in workplace contexts–as opposed to leisure contexts–there will be social structures in place that could make a relevant difference to whether (an increased degree of) surveillance can be justified. Likewise, the type of data that is collected (e.g., intimate, identifiable, health-related information in healthcare) may affect the analysis of whether increased surveillance is ethically permissible or ethically problematic, as well as the types of accountability structures that would be appropriate. We will return to this point in "Section IV: The need for accountability and oversight".

Second, it should be noted that, with few exceptions, the digital services we referenced already existed before the pandemic. As such, it may be questioned whether the increase of data collection resulting from various home confinement and social isolation measures by the private parties offering these services makes a qualitative difference in comparison to how it was before the pandemic. We cannot do full justice to this question, as the differences between contexts may lead to different answers, but we would like to make a general point that goes some way towards a positive response. The pandemic-related public health measures created a situation in which individuals, including those who had never used these services before, saw themselves compelled to join the trend towards remote working, online entertainment, and online retail. The emergency status of the pandemic inspired an attitude of hard work and sacrifice ("we all have to do our part") aimed at re-establishing a sense of normalcy (e.g., continuing work, still getting together (virtually) with friends to play games, etc.), that invited, nudged, or mandated people to use (a subset of) these services. This meant that these private actors had, as a result of the public health measures, a larger, wider, and more diverse audience than they otherwise would have had; an audience that they could–either directly or through the sale of advertisement placement–target with, say, product recommendations or political campaign ads. Having a substantially larger audience could thus mean substantially more influence on individuals as well as on societal processes. Moreover, in many cases, there would have been an expansion of the amount of data that was collected per individual, which means these private parties could uncover more individual behavioural patterns, idiosyncrasies, and susceptibilities, which they could, in principle, exploit for their own purposes (e.g., offering targeted, persuasive discount messages at specific times to increase sales). Now, we do not mean to claim that the corporations who facilitated society's needs during lockdowns, in fact, misused their position. Instead, what we are pointing to is that the shift towards online providers brought with it a shift in informational power, and that this shift in turn has implications for accountability.

Third, our examples would suggest that, in certain contexts and under certain conditions (including people's health, employment status, social environment, etc.), some (groups of) people would have consented to terms of service they would not have agreed to were it not for the pandemic and the public health response to the pandemic. Moreover, even the people who had consented to the terms of service before the pandemic, may not have anticipated the sheer volume of data and the corresponding behavioural patterns they would share with these parties. This points to difficult questions about the role, value, and voluntariness of (one-time) informed consent in these cases (see, e.g., Andreotta et al., 2022; Gefenas et al., 2022). At the same time, we recognize that, in some instances, for some individuals and for some services, informed consent may sufficiently protect these individuals' interests. Our aim here is to look at the bigger picture and show that the shifts towards online providers are best seen not as coincidental changes in consumption preferences, but rather as part of a pattern in which private companies essentially assumed or were granted the role of essential service provider (much like power or water suppliers). This wider view has implications for informational power and accountability, which we will discuss below.

To reiterate, the aim here is not to question the legality of the digital services offered by these companies, nor is it to admonish consumers for their choices. Moreover, we do not want to suggest that such incidental surveillance is unable to be justified in general cases, or in specific circumstances. Rather, we want to inquire after the justification for, and societal desirability of the enduring power increases of private parties as a result of increased incidental surveillance resulting from governmental responses to the pandemic. Subsequently, in "Section IV: The need for accountability and oversight", we aim to initiate a discussion about the increased informational power of these private parties and the duties of governments to provide accountability mechanisms for and oversight over the ways in which this power is wielded. We turn to considerations about private power now.

Section III: Considerations about justifications and private power

From the observations about the increased surveillance by private actors in various domains, a general pattern can be discerned that looks like this. In response to the pandemic, governments implemented liberty-restricting measures in

[12] We thank the two anonymous reviewers for pressing us to make this point explicitly.

service of public health. These effectively created urgent practical problems in need of solving (e.g., how to continue providing healthcare, education, etc.). Organizations and individuals alike looked for solutions to these problems and found them in existing, tried-and-tested commercially available solutions. Given the urgency of the situation, and the scarcity of non-commercial (e.g., government-run or non-profit) alternatives, the additional data disclosure—insofar as it was explicitly considered—was accepted as a necessity.

What such a stylized narrative about societal dynamics and psychological mechanisms offers is an *explanation* of the turn of events that led to the increase of incidental surveillance. The fact that organizations and individuals were put in a position in which they had to rapidly find solutions to the practical problems caused by the public health measures, including how to remain economically viable and societally relevant, *explains* why many organizations opted to outsource the management of remote communication and collaboration tools to experienced commercial parties, and why employees of these organizations in turn had little choice but to disclose data to these commercial parties. It also suggests that the limitations that lockdown measures placed on people's liberty to choose leisure activities (e.g., to meet with friends and family, to visit the cinema, to go to concerts or sporting events, etc.), *explains*, at least in part, their decision to use certain entertainment and retail services.[13]

Now, it may be that better, more nuanced explanations for the rise of incidental surveillance can be thought of, but that is beside the point. What we want to draw attention to is that having an explanation of a phenomenon does not mean the phenomenon is *justified* (cf. Nelson, 1986). That is, even if an account of the dynamics between public and private entities against a backdrop of existing societal structures helps provide an understanding of why things happened in the way they did, it may still be asked, from a normative standpoint, whether they *should* have.

More concretely, this means that even if a plausible explanation can be given of why governments allowed private actors to increase incidental surveillance in return for the use of services and infrastructure (e.g., an explanation in terms of expediency), it may be questioned whether this was the right trade-off to make. This is of course not to say that a justificatory story *cannot* be given, but rather to point out that thus far it has not been provided explicitly.

What governments have given are justificatory accounts of the instigating public health measures themselves; mostly in terms of the protection of public health and the principle of solidarity (e.g., Moss & Sandbakken, 2021; Pattyn et al., 2021). But this is only part of the story needed to justify incidental surveillance. First, as emphasized before, the surveillance we are interested in here is *incidental* to the COVID-19 pandemic public health measures. While direct pandemic surveillance is potentially justifiable by reference to public health reasons, the incidental surveillance is not necessarily nor immediately justified by the same public health reasons. If a person's personal movements and behaviours need to be known as part of contact tracing, that reason does not justify the surveillance of one's entertainment habits in order to increase company profits. That is, direct COVID-19 surveillance makes its justifications by reference to public health, whereas indirect surveillance of one's entertainment choices makes its justifications by reference to a company's responsibility to shareholders, stakeholders, or the like. The two justifications differ, and in this case, differ significantly.

A second part of this story is whether, from a normative point of view, the particular surveillance actors should have the authority to conduct such surveillance. Government surveillance, insofar as it can be justified, is typically justified by reference to the social contract and the responsibility of governments to provide security to its citizens.[14] In contrast, another mechanism must be found that grants private actors the authority to engage in such incidental surveillance. One such mechanism is that the subjects of surveillance have consented to surveillance, but as we already mentioned, when people are prohibited from leaving their homes but expected to work from home, keep the household running, and facilitate the remote schooling of children, it may be questioned whether consent to the various online services was informed and given voluntarily. Our more general point here, however, is that it needs to be critically assessed whether private companies' authority to conduct incidental surveillance was justified.[15]

Furthermore, it is important to note that increases of incidental surveillance by private actors cannot be justified by governments by appealing to necessity. After all, as certain subgroups of the population may attest (e.g., certain pensioners), it is possible, under favourable conditions—financial,

[13] For example, fervent soccer fans who were denied the opportunity to watch their favourite team live in the stadium, may have seen no alternative but to purchase a subscription to a premium soccer channel to follow their team. Or, perhaps more straightforwardly, people may have found themselves purchasing a subscription to a video content provider in the hopes of countering the dreariness of staying in during lockdown.

[14] We note here that the social contract, rights forfeiture, and the government's responsibility to provide security to its citizens are all contested and controversial areas. Moreover, we want to make it explicit that considerations about providing security to citizens does not immediately justify government surveillance. For example, see Henschke (2021).

[15] Notice, once more, that we are not here questioning the *legitimacy* of these private parties as such. Rather, we are inquiring after a justification for the major increases in incidental surveillance by private parties resulting from governmental responses to the pandemic.

social, and otherwise—to stay at home and practice social distancing for the sake of solidarity and the promotion of public health without being the subjects of direct or incidental surveillance. Moreover, it would have been possible for governments to offer financial compensation to organizations who deployed non-commercial communication tools, or for supranational institutions like the European Commission to instantiate non-profit, privacy-preserving communication platforms.[16] Had they done so, the situation may have been different. Since governments did take precautions to minimize governmental surveillance, the onus lies with them to justify why they have not taken additional steps to protect their citizens from increased incidental surveillance by private actors as a result of the lockdown measures they implemented.

These justificatory discussions matter due to the informational power that private companies have as a result of incidental surveillance. While the information gathered in this incidental surveillance varies in content and degree of ethical significance—after all, healthcare data gathered from telemedicine is of a different kind to the data that entertainment companies collect—they are all ethically relevant because of the informational power they grant the respective private actors. That is, the information arising from incidental surveillance, including the information emerging from aggregation and analysis,[17] places these private parties in privileged positions from which they can help or harm individuals, and support or disrupt societal structures.

In relation to the individual, consider again incidental surveillance arising in the workplace. By tracking their online activities (e.g., the duration of their use of Microsoft Word, Excel, and Teams), an employer may now be able to put pressure on an employee to work longer hours, or engage in a wider range of tasks because they know more about the employee's working habits. Vice versa, the employer could also use their gained informational power to assess which employees seem overburdened or have an unevenly distributed workload.

In relation to society more broadly, the informational power that corporations gained typically manifests itself as derived economic and market powers. The market value of remote entertainment providers, for example, rose during the first two years of the COVID-19 pandemic not only because there were more customers buying access to their services and products. These company's market value is derived, in part, from the fact that they gather large amounts of information on user habits, which they aggregate and analyse to glean potential insights into users and products that they can then monetize. The informational power derived from incidental surveillance thus leads to increased economic power. But note that behavioural analyses of user data can serve other derived purposes too, as illustrated by various cases in which surveillance data arising from entertainment services, specifically social media, were used for political purposes or ends (for an example, see the discussion of the Cambridge Analytica scandal in the next section). Because surveillance information can serve different purposes (Henschke, 2017), it grants informational power across a range of spheres of influence.

The overall point of this section is to show that justifications matter. The rise of incidental surveillance during the COVID-19 pandemic has led to a shift in, and increase in, private informational power. While the collection and use of surveillance information might be justifiable, different justifications may be needed depending on who is performing the surveillance and why. To look to government use of surveillance information as being justified by reference to public health reasons is not enough. Incidental surveillance by private actors requires a different set of justifications. The implications of changing informational power and the need to justify it in relation to incidental surveillance are discussed in the final section of this paper.

Section IV: The need for accountability and oversight

This brings us to the final aim of this paper, namely to examine the governance implications of the increased reliance on private actors for providing and maintaining certain infrastructure and services, and the de facto increase in incidental surveillance by private actors. Supposing that our claims are true, what is in the balance, and how do we, as a society, want to proceed?

A first observation is that what we refer to as "incidental surveillance" is by no means "accidental surveillance". As surveillance scholars have pointed out, controlling the flow of information is increasingly important in our current economic system to gain power over people and institutions, and to direct behaviour (*surveillance capitalism;* e.g., Zuboff, 2019; Henschke, 2022). Seen in this light, the increase of surveillance by private actors that we describe is not mere happenstance resulting purely from the turmoil of the pandemic. Nor, on this perspective, should the absence of non-commercial digital infrastructures and government-run communication platforms be considered an unfortunate contingency.[18] Rather, there are major political

[16] Practically, taking such measures would in all likelihood not have been straightforward, but that is also not our claim. The point is only that governments could have responded differently than they did.

[17] For more on this, see Solove (2004), Henschke (2017), and Nissenbaum (2009).

[18] It may be objected that governments, at the beginning of the pandemic, simply did not have the means to quickly replicate the large-

and economic forces at play, including neoliberalist ideals about deregulated, free markets and small governments, that work in concert towards the transfer of informational power from governments to a relatively small number of public and private entities. This process, which Henschke (2022) has called the "oligopologisation" of informational power, diffuses informational power and thereby weakens the position of governments.

Whether such a development in itself should be deemed problematic is contestable, with the debate involving a multitude of nationally and culturally dependent considerations, including the current form of government, the level of political trust, the presence (or absence) of privacy-related legislation, and the extent to which citizens can exercise their human rights.[19] It is worth noting, therefore, that making claims in favour of one direction or the other is beyond the scope of this paper. Rather, what we wish to emphasize here is the more general point that informational power, when left unchecked, can have severely negative consequences for society, for example by disrupting the relations between citizens and state (cf. Henschke, 2022).

As an illustration, consider the way in which Cambridge Analytica, a daughter company of the SCL group, used the informational power they had gained by illicitly scraping people's Facebook data to influence the 2016 U.S. presidential election (Isaak & Hanna, 2018). Or consider the role social media played in targeting individuals with propaganda and "fake news" that led to the 2021 U.S. capitol riots (Riley, 2022). Or, to give a slightly different example, consider how the lack of transparency ("opaqueness") inherent in bulk data collection and subsequent algorithmic processing by private parties have led to citizens being unfairly disadvantaged by automated decision making without the opportunity to inspect and appeal the underlying reasoning (e.g., Ferrer et al., 2021; Obermeyer et al., 2019; see also Robbins & Henschke, 2017).

This leads to a second observation, which is related to but distinct from the first, namely that power requires accountability and oversight. As noted in "Section I: Terms and concepts", accountability is more encompassing than oversight. Whereas oversight is concerned with the review and evaluation of selected activities, accountability involves an "account giver" offering an explanation for their activities, and a particular forum passing judgment on that explanation (and potentially bringing about consequences if the explanation is not deemed to be sufficient).

In liberal democracies, it is generally held that states need to have processes that *ensure* protection from authoritarianism and *assure* the public of these protections (Robbins & Henschke, 2017). In the context of surveillance, this means that governmental agencies in liberal democracies that engage in bulk data collection must both ensure that such data collection is justified, and offer the public justifications for this to assure the public that the data collection is done in a way that is best practice.[20] One partial explanation for this is the social contract—in recognition of the power that the state has over its citizens, governments owe those citizens mechanisms to ensure and assure that such power is used appropriately. That is, mechanisms of accountability are necessary for the social contract to remain valid. As Iyad Rahwan notes, modern forms of the social contract follow Jean Jac Rousseau, in which "the sovereign implements the *general will*… of the people, and is held in some way accountable for violations of fundamental rights" (author's original emphasis; Rahwan, 2018, p. 8). The particular mechanisms that ensure accountability will differ, but regular, open, free, and fair elections are one obvious mechanism to ensure such accountability.[21]

For those less convinced of the social contract, accountability can also be expounded in terms of power and fairness. If one party has power over another, then it is simply in the interests of the other party to know how that power is being wielded and why. Either way, liberal democracies devote significant resources to ensuring and assuring their citizens that power is not being abused. To this end, typical governmental surveillance is subject to significant formal processes of oversight and accountability (Lester, 2015). Moreover, there are a range of informal social norms that can, and should be, inculcated in governmental surveillance practices to ensure they are justified and proportionate to those justifications (Henschke, 2018, 2021).

While there are major national differences in how accountability for surveillance activities is regulated and enforced, and these mechanisms have frequently been found inefficient or malfunctioning (cf. Gill, 2020), there does seem to be a systematic difference in how governmental agencies are held accountable compared to private actors. State intelligence agencies, for example, are typically subject to significantly more stringent constraints than private information companies (Henschke, 2022; Lester, 2015).

Footnote 18 (continued)

scale digital infrastructure required for remote working. That may be true, but the point to notice is that this is the result of prior political choices.

[19] In authoritarian regimes, for example, shifts in informational power to private actors (i.e., the availability of social media platforms) may empower minorities to speak out and challenge authoritarian practices (Abbott, 2012).

[20] As a recent example, consider how various EU member states wanting to implement "digital contact tracing" technologies converged to decentralized systems with anonymous, rolling proximity identifiers after public debate about how to best design such apps in a privacy-preserving way.

[21] For a partial taxonomy of available accountability mechanisms, see Mashaw (2006).

Private actors, in contrast, are typically (and historically) left free to significant extents to pursue their economic ends, including mining and selling various forms of data, provided they have the consent of their customers and stay within the boundaries of the (locally applicable) law. This is especially true in non-European countries like the United States, where there is no unified data protection regulation in place and data protection is regulated differently for public and private entities (Levin & Nicholson, 2005).

Such regulatory differences between the public and private spheres can, in general terms, be traced to governmental commitments of non-interference aimed at limiting the influence of the state on both individual lives (i.e., negative obligations to refrain from infringing on human rights) and market dynamics (i.e., commitments to open, competitive markets in which the laws of supply and demand operate with no or limited governmental intervention). These commitments essentially pull in different directions: on the one hand, commitments to non-interference in people's personal lives pull in the direction of creating accountability structures that protect individuals from undue interference by public actors; on the other hand, commitments to non-interference in the marketplace pulls in the direction of letting private actors in their respective markets regulate themselves.

In recent years, following economic and financial crises, and in response to digital innovations, many democratic states have come to realize that some degree of market regulation is needed for most markets for them to function properly and to protect consumers from various malpractices (Cafaggi & Renda, 2012). However, the degree to which such protections are offered in different legal contexts varies substantially, and frequently, developments in the direction of governmental market regulation are actively opposed by corporate lobby groups and free market advocates who favour self- and co-regulatory solutions (Saurwein, 2011). As a result, even in the EU, which has some of the strongest consumer protection laws like the General Data Protection Act (GDPR), the Digital Services Act (DSA) and the Digital Markets Act (DMA), there remain asymmetries between how public and private actors are regulated.

In the context of the COVID-19 pandemic, regulatory asymmetries could be observed between, on the one hand, governmental agencies who engaged in direct COVID-19-related surveillance, and, on the other hand, private parties who increased their surveillance as a result of COVID-19 public health measures. Most liberal democratic states placed limitations on the various government departments that could access pandemic surveillance data. For instance, in Australia, police were prevented from accessing QR code check-in data for non-COVID-19 surveillance purposes (Greenleaf & Kemp, 2021). These efforts were recognised and responded to by actors like the Australian Information Commissioner, and various state law makers, who suggested more active oversight and accountability in relation to direct COVID-19 surveillance. In the Netherlands, temporary legislation was drafted to provide a legal basis for the use of the national contact tracing app "CoronaMelder", appoint oversight bodies and stipulate explicit limitations to data collection and data use. In contrast, the private companies who engaged in incidental surveillance were by and large allowed to increase their surveillance without any comparable changes in accountability or oversight.[22]

There is reason, however, to question whether this difference should be upheld in relation to the large tech companies that we are considering. As was underlined by the COVID-19 pandemic, private digital infrastructure and services have become critical for facilitating processes that sustain the functioning of society (cf. Aradau, 2010). Institutions and individuals became increasingly dependent on that infrastructure and the provision of those services, to the point that they would be at a considerable disadvantage if they did not have access to them. Functionally, then, the private actors responsible for maintaining the relevant infrastructure and digital services acted as *essential service providers*, comparable to governmental agencies responsible for water and wastewater management, energy provision, public transportation, and public infrastructure.[23]

This essential services perspective suggests that the de facto dependency between states and these digital service providers is not an informal and non-committal relationship, but resembles a public–private partnership (Pongsiri, 2002). This indicates that these service providers, in certain contexts and under specific conditions, have responsibilities to ensure that the use of these services is attainable for all who wish to make use of them, that the services are of a certain quality, and that the infrastructure and services are

[22] Critical questions were asked by authors like Tamar Sharon of the Google/Apple partnership that was formed to facilitate the development of digital contact tracing apps (e.g., Sharon, 2021). As the surveillance that would potentially have stemmed from this development would largely have been within the context of COVID-19 surveillance, we do not consider the Google/Apple partnership an example of incidental surveillance. However, our general point about the need for accountability structures to curtain the power of private actors very much aligns with Sharon's overarching concern that large tech companies are accumulating power across decision-making spheres with insufficient accountability.

[23] There are good reasons to think services that allow for employment and access to entertainment are ethically significant in that employment and access to entertainment are potentially human rights. For instance, Article 23 of the United Declaration of Human Rights states that "[e]veryone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment" and Article 27 states that "[e]veryone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits."

reliably available. Vice versa, it implies that governments have duties to the public to ensure that these private actors indeed deliver the critical services and maintain the infrastructure. Importantly, it also suggests that governments have a role to play in regulating and providing oversight over the surveillance activities of these actors to secure and protect the privacy of all citizens, including those who have no choice but to rely on these services.

Based on this perspective, we submit as a guiding principle that the corporations providing essential services should at least be held to same standards of oversight and accountability as comparable governmental agencies that are tasked with surveillance, especially in times of crisis. Certainly, the bodies responsible for oversight may be different, and the details of the accountability processes for public or private actors could come apart, but the level of protection offered to individuals should, in principle, be comparable.

This suggestion entails challenging conceptual and practical matters that will need to be addressed, most likely in national or supranational contexts, including determining which private parties could reasonably be said to function as essential service providers, what governmental bodies or independent institutions would be most suitable to be tasked with oversight, and what accountability structures would be appropriate in a given context.[24] Drawing a parallel with the structures that are applicable in the public domain, these accountability structures would, in broad terms, need to ensure that the increased informational power stemming from incidental surveillance is either justified by a non-public health reason or limited when those justifications are no longer compelling. Moreover, the accountability structures would need to assure account keepers and other relevant stakeholders that any such changes meet societal standards.

Though the specific characteristics of the different contexts and the different legal systems which govern those contexts will co-determine which accountability structures are appropriate, options include instantiating more extensive (algorithmic) transparency obligations, mandating opt-in rather than opt-out policies for data use and resale, prescribing accessible review and complaint procedures, and strengthening possibilities for sanctions and remedial action. Other possibilities include directives to limit the for-profit use and resale of data profiles that were created during public health emergency measures such as lockdowns, or to require service providers to ask people who subscribed to an online service during a lockdown to reconfirm their consent after the lockdown ended. More stringent reporting, monitoring and documentation requirements could also be considered.

For guidance, it will be instructive to review the "Guiding Principles on Business and Human Rights (UNGPs)," endorsed in 2011 by the UN Human Rights Council, which outline the corporate responsibilities businesses have to protect human rights (including the right to privacy).[25] Another relevant development in this space is the European Commission's proposal for a Corporate Sustainability Due Diligence Directive (CSDDD), which aims to require EU companies and non-EU companies operating in the EU to establish due diligence procedures to address potential adverse impacts of their actions–as well as the actions of their subsidiaries and business partners located in and outside of the EU–on human rights. At present, the directive is under negotiation, but if this directive comes into effect, it will strengthen corporate accountability for human rights, including privacy, in the EU and beyond. Moreover, if adopted, the directive may set a precedent for other countries as well to create a legal basis for more corporate accountability.

Given the complexities involved, there is a clear need for further research and broad legislative debate about incidental surveillance and its implications for society. Our contribution has been (1) to foreground the phenomenon itself, (2) show that justifications have so far been lacking for the resulting increase in surveillance, and, (3) through an argument of consistency, suggest that the private parties who functionally fulfill a role akin to a public service provider–at least during public health emergencies–may need to be subjected to accountability structures and oversight mechanisms on par with those applicable to public actors engaging in surveillance.

Conclusions

As we have discussed, the COVID-19 pandemic has given rise to a special situation in which certain surveillance practices, including the sharing and analysing of Google location data and cell tower information, were deemed necessary for reasons of public health. Many people accepted surveillance due to the real and significant risks faced by individuals, communities, and indeed governments, by COVID-19. However, as we have argued, the surveillance that arose *incidentally* to the public health measures is not automatically justified by the same justifications. To reiterate, the point is not that no such justifications could be given, but rather that important work remains to be done with regard to assessing, with respect to specific legal and societal contexts, the

[24] The suggested principle also points to a larger debate pertaining to general accountability concerns associated with governments 'contracting out' certain activities to private parties. This debate is better left to legal and public policy scholars, but for an overview of some of the difficulties, see Mashaw (2006), especially pp. 134–138.

[25] For an excellent discussion on the implications of the UNGPs on corporate accountability, see Bernaz (2020).

desirability and permissibility of the shifts in informational power we have identified.

Of course, if it turns out that the increased incidental surveillance cannot be (wholly) justified, there will be difficult practical issues to resolve, for example about developing alternative revenue models for the corporations that provide critical infrastructure but currently rely predominantly on data mining to remain financially solvent.[26] Alternatively, if political choices are made to shift certain responsibilities to public agencies, there may be issues concerned with the design, development, and maintenance of large-scale, privacy-preserving alternative services in the public domain. But the prospect of having to deal with these complex challenges should not deter from having a public debate about the desirability of having the critical digital services and infrastructure that individuals and institutions are required to rely on be paid for with the private and personal data of citizens.

Relatedly, and much along the same lines, we have argued that, given the increased informational power that private actors have in fact accrued as a result of the public health measures instituted and enforced by governments around the world, there is an increased need for oversight and for mechanisms for holding these private actors accountable for the way they collect, process, and potentially monetize the data flowing from their surveillance practices. With confidence among experts growing that zoonotic viruses like SARS-CoV-2 will be among us for years to come, and that lockdowns and isolation measures will remain effective public health interventions when new disease outbreaks occur, the time for the debate about incidental surveillance is now.

Finally, we suggest that our paper has implications that are wider than the context of COVID-19, or even public health responses more generally. As the internet has generally made us more dependent on information and communications infrastructures, and private actors are in fact essential for maintaining those infrastructures and for providing (or preventing) access to crucial digital services on top of those infrastructures, questions about oversight and corporate accountability are becoming increasingly urgent. In order to ensure and assure that the increased informational power by private actors is not abused, we must be vigilant in checking and assessing the justifications for such power.

Acknowledgements This work is part of the research programme Ethics of Socially Disruptive Technologies, which is funded through the Gravitation programme of the Dutch Ministry of Education, Culture, and Science and the Netherlands Organization for Scientific Research (NWO Grant Number 024.004.031). We thank Sylvia Karlsson-Vinkhuyzen for thoughtful comments on an earlier draft of the manuscript. We are grateful to Nadia Bernaz for her suggestions on how to improve the paragraphs on corporate accountability.

Funding The authors did not receive any specific funding for this project.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Competing interests Not applicable.

References

Abbott, J. (2012). Democracy@ internet org Revisited: analysing the socio-political impact of the internet and new social media in East Asia. *Third World Quarterly, 33*(2), 333–357.

Andreotta, A. J., Kirkham, N., & Rizzi, M. (2022). AI, big data, and the future of consent. *AI & Society, 37*(4), 1715–1728.

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue, 41*(5), 491–514.

Bernaz, N. (2020). Conceptualizing corporate accountability in international law: Models for a business and human rights treaty. *Human Rights Review, 22*(1), 45–64.

Blasimme, A., Ferretti, A., & Vayena, E. (2021). Digital contact tracing against COVID-19 in Europe: Current features and ongoing developments. *Frontiers in Digital Health, 3*, 61.

Bloem, B. R., Dorsey, E. R., & Okun, M. S. (2020). The coronavirus disease 2019 crisis as catalyst for telemedicine for chronic neurological disorders. *JAMA Neurology, 77*(8), 927–928.

Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems, 21*(4), 234–246.

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal, 13*(4), 447–468.

Cafaggi, F., & Renda, A. (2012). Public and private regulation: Mapping the labyrinth. *The Dovenschmidt Quarterly*, 16.

Coghlan, S., Miller, T., & Paterson, J. (2021). Good proctor or "big brother"? Ethics of online exam supervision echnologies. *Philosophy & Technology, 34*(4), 1581–1606.

ConSalud. (2020). El uso de la telemedicina en España aumenta un 153%. Retrieved November 23, 2022, from https://www.consalud.es/tecnologia/tecnologia-sanitaria/telemedicina-espana-aumenta-153_78862_102.html

Curry, D. (2022). Microsoft Teams Revenue and Usage Statistics. Retrieved November 23, 2022, from https://www.businessofapps.com/data/microsoft-teams-statistics/

[26] For example, perhaps governments could pay a fixed fee for each individual who chooses to opt out of being tracked when using a particular, privately-run critical service during periods of lockdown.

Espiner, T. (2020). Covid-19: Nintento profits triple as games boom continues. Retrieved November 23, 2022, from https://www.bbc.com/news/business-54813841

Fazio, M. (2021). Plastic Surgeon Attends Video Traffic Court From Operating Room. In *The New York Times*. Retrieved November 23, 2022, from https://www.nytimes.com/2021/02/28/us/california-surgeon-zoom-traffic-violation-court.html

Ferrer, X., van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: A cross-disciplinary perspective. *IEEE Technology and Society Magazine, 40*(2), 72–80.

Gefenas, E., Lekstutiene, J., Lukaseviciene, V., Hartlev, M., Mourby, M., & Cathaoir, K. Ó. (2022). Controversies between regulations of research ethics and protection of personal data: Informed consent at a cross-road. *Medicine, Health Care and Philosophy*, 1–8.

Gerli, P., Arakpogun, E. O., Elsahn, Z., Olan, F., & Prime, K. S. (2021). Beyond contact-tracing: The public value of eHealth application in a pandemic. *Government Information Quarterly, 38*(3), 101581.

Gerlitz, E., & Häring, M. (2023). Privacy research on the pulse of time: COVID-19 contact-tracing apps. In *Human factors in privacy research* (pp. 219–235). Springer.

Gill, P. (2020). Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security, 35*(7), 970–989.

Grantz, K. H., Meredith, H. R., Cummings, D. A., Metcalf, C. J. E., Grenfell, B. T., Giles, J. R., Mehta, S., Solomon, S., Labrique, A., Kishore, N., Buckee, C. O., & Wesolowski, A. (2020). The use of mobile phone data to inform analysis of COVID-19 pandemic epidemiology. *Nature Communications, 11*(1), 1–8.

Greenleaf, G., & Kemp, K. (2021). Australia's 'COVIDSafe'law for contact tracing: An experiment in surveillance and trust. *International Data Privacy Law, 11*(3), 257–275.

Henschke, A. (forthcoming). The dynamics of public health ethics: COVID-19 and surveillance as *justifiable but abnormal*. In K. Macnish, & A. Henschke, (Eds)., *The ethics of surveillance in times of emergency*. Oxford University Press.

Henschke, A. (2017). *Ethics in an age of surveillance*. Cambridge University Press.

Henschke, A. (2018). Conceptualising proportionality and its relation to metadata. In D. Baldino & R. Crawley (Eds.), *Intelligence and the function of government.* Melbourne University Press.

Henschke, A. (2021). From Need to share to need to care: information aggregation and the need to care about how surveillance technologies are used for counter-terrorism. In J. Feltes, A. Henschke, & S. Miller (Eds.), *Counter-terrorism: The ethical issues.* Edward Elgar.

Henschke, A. (2022). Information as an evolving national security concern. In M. Clarke, A. Henschke, M. Sussex, & T. Legrand (Eds.), *The Palgrave Handbook of National Security* (pp. 389–408). Palgrave Macmillan.

Ipsen, C., van Veldhoven, M., Kirchner, K., & Hansen, J. P. (2021). Six key advantages and disadvantages of working from home in Europe during COVID-19. *International Journal of Environmental Research and Public Health, 18*(4), 1826.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56–59.

Jameda Pressemitteilungen. (2020). Covid-19 führt zu steigender Nachfrage nach Videosprechstunde. (Covid-19 leads to increasing demand for video consultations), 30 March 2020.

Kamphorst, B. A., & O'Neill, E. (in prep.). Digital recording and the hazards of unbounded moralized judgment. [Manuscript in preparation].

Kamphorst, B. A., Verweij, M. F., & van Zeben, J. A. (2023). On the voluntariness of public health apps: A European case study on digital contact tracing. *Law, Innovation and Technology, 15*(1), 107–123.

Kharbat, F. F., & Abu Daabes, A. S. (2021). E-proctored exams during the COVID-19 pandemic: A close understanding. *Education and Information Technologies, 26*(6), 6589–6605.

Latheef, S. (forthcoming). Digital Contact Tracing Applications (DCTAs); is it the end of informed consent and autonomy. In K. Macnish & A. Henschke (Eds.), *The ethics of surveillance in times of emergency*. Oxford University Press.

Lau, J., Knudsen, J., Jackson, H., Wallach, A. B., Bouton, M., Natsui, S., Philippou, C., Karim, E., Silvestri, D. M., Avalone, L., Zaurova, M., Schatz, D., Sun, V., & Chokshi, D. A. (2020). Staying connected in the COVID-19 pandemic: Telehealth at the largest safety-net system in the United States: A description of NYC Health+ Hospitals telehealth response to the COVID-19 pandemic. *Health Affairs, 39*(8), 1437–1442.

Lester, G. (2015). *When should state secrets stay secret? Accountability, democratic governance, and intelligence*. Cambridge University Press.

Levin, A., & Nicholson, M. J. (2005). Privacy law in the United States, the EU and Canada: The allure of the middle ground. *U. Ottawa l. & Tech. J., 2*, 357.

Lukas, H., Xu, C., Yu, Y., & Gao, W. (2020). Emerging telemedicine tools for remote COVID-19 diagnosis, monitoring, and management. *ACS Nano, 14*(12), 16180–16193.

Lyon, D. (2009). Surveillance, power, and everyday life. In C. Avgerou, R. Mansell, D. Quah, & R. Silverstone (Eds.), *The Oxford handbook of information and communication technologies.* Oxford University Press.

MacDonald, K. I. (1976). Is 'power' essentially contested? *British Journal of Political Science, 6*(3), 380–382.

Macnish, K. N. J., & Henschke, A. (Eds.) (forthcoming). *Surveillance in times of emergency.* Oxford University Press.

Mann, D. M., Chen, J., Chunara, R., Testa, P. A., & Nov, O. (2020). COVID-19 transforms health care through telemedicine: Evidence from the field. *Journal of the American Medical Informatics Association, 27*(7), 1132–1135.

Mashaw, J. L. (2006). Accountability and institutional design: Some thoughts on the grammar of governance. *Public Law Working Paper* (116), 115–156.

Masoni, M., & Guelfi, M. R. (2020). WhatsApp and other messaging apps in medicine: Opportunities and risks. *Internal and Emergency Medicine, 15*(2), 171–173.

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2022). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, 1–53.

McGreevey, J. D., Hanson, C. W., & Koppel, R. (2020). Clinical, legal, and ethical aspects of artificial intelligence–assisted conversational agents in health care. *JAMA, 324*(6), 552–553.

Microsoft. (2022). Microsoft 365 usage analytics. Retrieved November 2, 2022, from https://learn.microsoft.com/en-us/microsoft-365/admin/usage-analytics/usage-analytics?view=o365-worldwide

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the internet. *Journal of Business Ethics, 28*(3), 255–265.

Moss, S. M., & Sandbakken, E. M. (2021). "Everybody needs to do their part, so we can get this under control." reactions to the Norwegian government meta-narratives on COVID-19 measures. *Political Psychology, 42*(5), 881–898.

Nelson, A. (1986). Explanation and justification in political philosophy. *Ethics, 97*(1), 154–176.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nye, J. S., Jr. (2004). *Soft power: The means to success in world politics*. Public Affairs.

Nye, J. S., Jr. (2011). *The future of power*. Public Affairs.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science, 366*(6464), 447–453.

Ogul, M. S., & Rockman, B. A. (1990). Overseeing oversight: New departures and old problems. *Legislative Studies Quarterly*, 5–24.

O'Neill, E. (2021). Digital Wormholes. *AI & Society*, 1–3.

O'Neill, E. (2022). Contextual integrity as a general conceptual tool for evaluating technological change. *Philosophy & Technology, 35*(3), 79.

O'Neill, O. (2004). Informed consent and public health. *Philosophical Transactions of the Royal Society of London Series B: Biological Sciences, 359*(1447), 1133–1136.

Pagliari, C. (2020). The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response. *Journal of global health*, *10*(2).

Parviainen, J., & Rantala, J. (2022). Chatbot breakthrough in the 2020s? An ethical reflection on the trend of automated consultations in health care. *Medicine, Health Care and Philosophy, 25*(1), 61–71.

Pattyn, V., Matthys, J., & Hecke, S. V. (2021). High-stakes crisis management in the Low Countries: Comparing government responses to COVID-19. *International Review of Administrative Sciences, 87*(3), 593–611.

Pongsiri, N. (2002). Regulation and public-private partnerships. *International Journal of Public Sector Management., 15*(6), 487–495.

Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. *Ethics and Information Technology, 20*(1), 5–14.

Rechtbank Amsterdam. (2020). Court case ECLI:NL:RBAMS:2020:2917. Retrieved November 23, 2022, from https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:2917

Richardson, E., Aissat, D., Williams, G. A., & Fahy, N. (2020). Keeping what works: Remote consultations during the COVID-19 pandemic. *Eurohealth, 26*(2), 73–76.

Riley, J. K. (2022). Angry enough to riot: An analysis of in-group membership, misinformation, and violent rhetoric on The Donald. win between election day and inauguration. *Social Media Society, 8*(2), 20563051221109188.

Robbins, S., & Henschke, A. (2017). The value of transparency: Bulk data and authoritarianism. *Surveillance & Society, 15*(3/4), 582–589.

Saurwein, F. (2011). Regulatory choice for alternative modes of regulation: How context matters. *Law & Policy, 33*(3), 334–366.

Shah, B. R., & Schulman, K. (2021). Do not let a good crisis go to waste: Health care's path forward with virtual care. *NEJM Catalyst Innovations in Care Delivery*, *2*(2).

Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology, 23*(Suppl 1), 45–57.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age* (Vol. 1). New York University Press.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Sweney, M. (2020). Lockdown drives UK TV streaming customers to more than 32m. In *The Guardian*. Retrieved November 23, 2022, from https://www.theguardian.com/tv-and-radio/2020/dec/27/netflix-amazon-and-disney-push-uk-to-more-than-32m-tv-streaming-customers

Tyrväinen, O., & Karjaluoto, H. (2022). Online grocery shopping before and during the COVID-19 pandemic: A meta-analytical review. *Telematics and Informatics, 71*, 101839.

Vargo, D., Zhu, L., Benwell, B., & Yan, Z. (2021). Digital technology use during COVID-19 pandemic: A rapid review. *Human Behavior and Emerging Technologies, 3*(1), 13–24.

Weise, K. (2021). Amazon's profit soars 220 percent as pandemic drives shopping online. In *The New York Times*. Retrieved November 23, 2022, from https://www.nytimes.com/2021/04/29/technology/amazons-profits-triple.html

Yeung, J. (2020). Sony's Q2 earnings reveal PS4 games rocketed 83% during COVID-19. Retrieved November 23, 2022, from https://hypebeast.com/2020/8/sony-q2-2020-earnings-playstation-4-game-sales-double-news

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