Check for updates

Original Research Article

BIG DATA & SOCIETY

Big Data & Society
July–December: 1–14
© The Author(s) 2020
DOI: 10.1177/2053951720976680
journals.sagepub.com/home/bds
SAGE

Innovation under pressure: Implications for data privacy during the Covid-19 pandemic

Gemma Newlands[1], Christoph Lutz[1], Aurelia Tamò-Larrieux[2,3], Eduard Fosch Villaronga[4], Rehana Harasgama[5] and Gil Scheitlin[6]

Abstract

The global Covid-19 pandemic has resulted in social and economic disruption unprecedented in the modern era. Many countries have introduced severe measures to contain the virus, including travel restrictions, public event bans, non-essential business closures and remote work policies. While digital technologies help governments and organizations to enforce protection measures, such as contact tracing, their rushed deployment and adoption also raises profound concerns about surveillance, privacy and data protection. This article presents two critical cases on digital surveillance technologies implemented during the Covid-19 pandemic and delineates the privacy implications thereof. We explain the contextual nature of privacy trade-offs during a pandemic and explore how regulatory and technical responses are needed to protect privacy in such circumstances. By providing a multi-disciplinary conversation on the value of privacy and data protection during a global pandemic, this article reflects on the implications digital solutions have for the future and raises the question of whether there is a way to have expedited privacy assessments that could anticipate and help mitigate adverse privacy implications these may have on society.

Keywords

Privacy, surveillance, Big Data analytics, data protection, pandemic, Covid-19, contextual privacy, coronavirus, health data, GDPR

Introduction

The Covid-19 pandemic has resulted in unprecedented social and economic disruption worldwide. Racing against an invisible enemy, a virus simultaneously foreign and ubiquitous, most governments have introduced drastic measures to curb its spread and flatten the curve. Time is of the essence during a pandemic (French et al., 2018; Milne and Costa, 2020), providing both governments and organizations with the moral license to take extraordinary measures, such as travel restrictions, bans of public gatherings, closures of non-essential businesses and transitions to remote work and education. A particularly striking characteristic of the Covid-19 pandemic has been the rapid deployment of novel digital technologies, such as contact-tracing apps (Ferretti et al., 2020). Society has also witnessed intensification in the use of pre-existing digital products, such as video-conferencing software. Receiving only limited exposure pre-pandemic, Zoom has become a household name and an essential component for parties (Matyszczyk, 2020), weddings (Pajer, 2020), school and work.

Governments, private companies and public organizations have traditionally all been involved in shaping

[1]Nordic Centre for Internet and Society, BI Norwegian Business School, Oslo, Norway
[2]FAA – Institute for Work and Employment Research, University of St Gallen, St Gallen, Switzerland
[3]Digital Society Initiative, University of Zurich, Zurich, Switzerland
[4]eLaw Center for Law and Digital Technologies, Leiden University, Leiden, The Netherlands
[5]Bär & Karrer Ag, Zurich, Switzerland
[6]Data Protection Department, University of Zurich, Zurich, Switzerland

Corresponding author:
Christoph Lutz, Handelshoyskolen BI Nydalsveien 37 Oslo, Oslo 0484, Norway.
Email: christoph.lutz@bi.no

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

norms for digital surveillance in Europe. Yet, during the Covid-19 pandemic, these digital technologies have been deployed ad-hoc without proper impact assessment, stakeholder consultation or evaluation (Frith and Saker, 2020; Madianou, 2020; Milan and Treré, 2020). Since many of these digital technologies are data-intensive, generating vast amounts of intimate biometric and location data (Taylor, 2020), concerns about their impact on privacy and data protection have been raised from civil rights advocates, policymakers and the news media (Dubov and Shoptaw, 2020; French and Monahan, 2020; Kitchin, 2020; Maalsen and Dowling, 2020; Morley et al., 2020).

Concerns centre around how the pandemic could be exploited as an opportunity to normalize governmental surveillance (French and Monahan, 2020), particularly into the domestic and biopolitical sphere (Algorithmwatch, 2020; Maalsen and Dowling, 2020; Vallee, 2020). There is a particular concern about 'surveillance creep' (Andrejevic and Gates, 2014; Cheung, 2020) and that rushed decisions may stay in place in the long run, as 'temporary measures have a nasty habit of outlasting emergencies' (Harari, 2020). Structural inequalities in data access and exposure also mean that there may be disproportionate privacy invasion on certain, disadvantaged, societal groups (Taylor, 2020). Such concerns are justified, since states of emergency often result in increased surveillance and a bypassing of individual rights (Bigo, 2006; Lyon, 2003; Topak, 2017; York and McSherry, 2020). A primary concern is the potential transfer of such information from telecommunication companies to law enforcement agencies (FDPIC, 2020a; Ghosh, 2020; Polish Government, 2020). Organizations such as Human Rights Watch fear that some of the technology being used to seize the pandemic could be equally used to trace rioters in massive protests, such as the protests arising from George Floyd's murder (Toh and Brown, 2020).

The deployment of new applications and the intensified use of existing technologies to tackle the Covid-19 pandemic do not happen in a regulatory vacuum and therefore, compliance with data protection law, in particular the EU General Data Protection Regulation (GDPR), and the general data protection principles (GDPR Article 5) is key to the successful deployment and adoption of these technologies. General data protection principles such as the principle of proportionality, the principle of purpose limitation and the principle of transparency set the stage for compliance of contact-tracing applications and video-conferencing tools with data protection law. These principles require developers of new or existing technologies to implement privacy-friendly options from the beginning ('privacy-by-design') and ensure that not more personal data is processed than necessary to trace contact with a person infected with Covid-19, that the data is not used for other purposes than curbing the spread of Covid-19, and that the use of any data collected with these new and innovative technologies is transparent to the users. Finally, the GDPR requires a person's consent to the processing of their health data (GDPR Article 9). These general privacy principles do not prohibit the surveillance measures currently taken by governments or organizations, but rather ensure the correct handling of the data once processed under the current circumstances (GPA, 2020).

Research has started to explore the spatiality of Covid-19, in terms of data collection and privacy (Frith and Saker, 2020; Poom et al., 2020), but has so far mostly overlooked the temporal nature of how such privacy-negating technologies are deployed and normalized. Given the speed and complexity of the pandemic's societal impacts, it is equally as challenging as it is essential to track the development and use of digital surveillance and review the impact of such technologies on society to ensure compliance with data privacy law in all contexts. In this paper, we, therefore, look at the temporality of the Covid-19 pandemic and how speed interacts with regulatory protection of privacy in Europe.

This article is divided into two main parts. After the introduction, we discuss the notion of rushed innovation and argue how rushed innovation can have negative implications in general and in terms of privacy protection. This second section, which focuses on the socio-technological aspects of rushed innovation, is divided into two subsections. The first subsection revolves around the rushed deployment of novel technological solutions, with contact tracing apps as a central case. The second subsection focuses on the rushed adoption of pre-existing technologies, with Zoom as the central case. These cases were, and remain, topics that all governments, as well as industrial players in Europe, have to deal with in connection with the curbing of the spread of Covid-19, while at the same time ensuring compliance with privacy law and related expectations. The second key section of the paper then focuses on regulatory aspects of rushed innovation, focusing on the EU general data protection framework (GDPR). This section examines whether this legal framework accelerates or slows down rushed innovation. We bring forward concerns relating to how the law allows introducing products and services in the market that have not followed appropriate assessment and do not demonstrate full legal compliance. The article ends with a collection of lessons learned and paths forward.

The socio-technological aspects of rushed innovation during the Covid-19 pandemic

We live in an age of hypertemporality and hypercompetition (Carillo, 2005). Acceleration, as theorized by sociologists such as Hartmut Rosa, is a key aspect of modernity (Rosa, 2013) and technical acceleration, describing the increased speed of technological innovation and goal-directed processes, goes hand in hand with the acceleration of social change (e.g. cultural and institutional norms) and the pace of life. Such acceleration is particularly visible in the tech industry, where speed acts as an important part of the business model, both among large tech companies and start-ups (Tromble and McGregor, 2019; Wajcman, 2019). Speed in technological innovation often leads to competitive advantage and network effects (Eisenhardt and Martin, 2000; Griffin et al., 2019; Kessler and Chakrabarti, 1996). Accordingly, many tech firms have embraced a technological solutionism and social engineering approach that is characterized by 'release early, release often' in its softer and more benign version (Raymond, 1999) and 'move fast and break things' in its more aggressive version (Taneja, 2019). Addressing the critical importance of speed, innovation frameworks such as the lean start-up approach explicitly aim at shortening development cycles through the quick development of prototypes or minimum viable products and have enjoyed widespread success in the business community (Ries, 2011).

Rapid innovation is particularly important in a crisis, not only so that companies can exploit market advantages in what Klein (2007) refers to as 'disaster capitalism', but so that life-, society- and economy-preserving solutions can be rolled out where needed. Acknowledging the subjective experience of time (Orlikowski and Yates, 2002), Calhoun (2010) emphasizes how urgency shapes our temporal framework in a crisis. Governments worldwide face criticism for acting too slowly and costing lives. The constant update of Covid-19 death statistics online, like a ticking doomsday clock, offers a stark reminder that nothing can ever happen quickly enough in a crisis. There is a growing societal anxiety for quick responses and quick action to solve some of the greatest world challenges (Leslie, 2020).

Experts have stressed how innovation in the field of pharmaceutical technology (Bryan et al., 2020) should be inspired by fast and frugal innovations (Harris et al., 2020). Indeed, within research and policy fields, there is currently a lively discussion about fast-tracking vaccine development. News of the Russian authorization of Sputnik V and the Chinese authorization of CanSino's vaccine for military use (Liu and Woo, 2020), as well as Sinovac's and Sinopharm vaccines for emergency use (Liu and Kim, 2020), have sparked widespread criticism among Western experts (Callaway, 2020). However, daily media coverage in Europe centres around when, not if, a vaccine will be ready, to the point that a temporary pause on the Oxford University/AstraZeneca vaccine trials in September 2020 led to front-page news.

However, rushing innovation comes with its own problems. For instance, Tromble and McGregor (2019) discuss a speed-oriented focus on Facebook as one reason for some of the adverse developments in recent years. Facebook encourages its employees 'to be creative, to experiment, to move quickly from one idea to the next. If something fails, that is no problem. They keep trying until something works' (p. 325). However, such a speed-oriented process prohibits a slower but more methodical approach – one which could anticipate better the vast negative social impacts of social media in recent years.

Rapid innovation and regulatory compliance also often make for poor bedfellows. As Harris et al. (2020) remark concerning fast innovation for the Covid-19 pandemic, '[i]t is sometimes necessary to forego high regulatory standards in order to rapidly address new demands at low cost'. Coined by Hermosilla (2020) to refer to pharmaceutical companies rushing through licensing processes to the detriment of the product, 'rushed innovation' is a useful concept to explain the trade-offs between innovation, market advantage and regulatory compliance.

While rushed innovation does not have to mean that privacy rights are infringed upon, it is indeed likely that other concerns such as functionality and usability will be prioritized. Public health tools, in particular, will require access to certain information and can impinge on one's privacy. Yet, as Gasser et al. (2020) state: '[p]rivacy risks vary depending on the purpose and data types used by a digital tool'. The privacy-invasiveness will depend on the granularity of the data obtained, the centralized access versus decentralized access to said data, the duration of access to said data, and the risks of identification. Because 'privacy risks can change and accumulate over time', it is critical to have a strong regulatory framework in place to address privacy issues caused by rushed innovation (Gasser et al., 2020: 5). However, at the same time during this pandemic, we can see a shift towards protecting public health over privacy across many levels while relation on different justifications for this shift. The overall goal – protecting public health – seems to coincide on all levels as long as the principles of purpose limitation, proportionality and transparency are ensured (European Commission, 2020).

In the following, we distinguish two forms of rushed innovation, which we call *rushed deployment* and *rushed*

adoption. Rushed deployment refers to the rapid roll-out of new solutions, while rushed adoption describes the widespread adoption of existing services, and sometimes their *re-appropriation*, in the wake of the pandemic. While we know that the boundaries between the deployment of new technologies and the adoption of existing ones are not always clear cut, the differentiation helps create a structure for analysis.

Rushed deployment of new solutions

Rising infection rates and spreading uncertainty have led government officials and private companies on an urgent search for technical solutions that could be deployed promptly and efficiently. In an effort to monitor the spread of the virus, government officials turned towards Big Data solutions, which promise to analyze aggregated mobility data to provide information about when and near whom individuals were at a given moment. Multiple countries have implemented such practices (Buckee, 2020). Some countries, including Germany (Dalg, 2020), Switzerland (Wyss, 2020) and Norway (Balsari et al., 2020), have mandated national emergency cooperation with telecommunication providers to track the flow of individuals, mainly to ensure that people are not gathering in large groups or to track persons who have tested positive for Covid-19. In Italy, authorities analyzed citizens' location data from their phones to determine how many people are following the government's lockdown order. They could also identify the average distances in which citizens move every day (Corriere Della Sera, 2020).

Two technical approaches have, so far, dominated the dash towards the development of contact tracing technologies: GPS methods of co-localization tracing and Bluetooth-based methods of proximity tracing (Leslie, 2020). These practices have been scrutinized by privacy scholars since governments and health authorities have not provided enough transparency about how the tracking works (Ghosh, 2020; Steiger, 2020). Although the accumulation of data within telecommunication companies is not new, and its privacy implications were predictable, disclosure to the government is a novel consequence. This raises concern about the so-called private/public surveillance partnership (Schneier, 2015), referring to government and corporations' cooperative effort to collect mass amounts of personal data. Such attempts can be observed in the UK, where Prime Minister Boris Johnson called on the technology industry to contribute in the fight against Covid-19 (Waterson, 2020).

Beyond monitoring, many countries have launched contact-tracing apps to limit the spread of Covid-19. Mobile applications offer various ways to collect and distribute Big Data (Lai and Flensburg, 2020: 1). Even though contact tracing apps were used before to track epidemics of Ebola (Sacks et al., 2015) and Tuberculosis (Ha et al., 2016), their adoption in a pandemic is new. Such voluntary applications (Cho et al., 2020; Parker et al., 2020) have surged across Europe, giving rise to a broad discussion about the benefits and risks of such contact tracing apps. Scholars have warned about the risk of growing function creep and have argued:

> that apps [. . .] should be evaluated in terms of the contextual integrity of information flows; in other words, the appropriateness of sharing health and location data will be contextually dependent on factors such as who will have access to data, as well as the transmission principles underlying data transfer (Vitak and Zimmer, 2020: 1).

An effort to comply with privacy standards was the decentralized Pan-European Privacy-Preserving Proximity Tracing application (PEPP-PT, 2020). This tool shows the potential of technology to protect privacy, thus 'reframing technology, broadly defined, no longer (only) as a threat to privacy, but as part of the solution space' (Gasser, 2016: 65). It tracks devices that have been in close proximity to each other by a periodically changing identifier and functions without relying on mobility data or any personal data, therefore being compliant with data protection regulation. While it implements a decentralized approach by initially saving those identifiers locally on the user's device, it still relies on a centralized database to inform others in case a user discloses a positive test result. Two protocols emerged that differ in what data is transmitted to the central database in case the users disclose a positive test result. While PEPP-PT requires the transmission of all encounters (i.e. a list of identifiers) to a central database, DP-3T only requires the app to transmit a representation of its own identifiers. Other users can then use those representations to locally compute whether they have been in physical proximity with an infected person (Troncoso et al., 2020). This approach 'ensures [that] personal data and computation stays entirely on an individual's phone' (Troncoso et al., 2020). It is an open-source approach that brings together competing interests, health and privacy, a trade-off not readily endorsed by others (Harari, 2020) and therefore, takes a privacy-by-design approach. A notable technical solution that has been initiated by the private side is the exposure notification API jointly developed by Apple and Google, which according to Google's Dave Burke, VP of Android engineering, is 'heavily inspired by the DP-3T group and their approach'

(Etherington and Lomas, 2020) and was received with support from privacy scholars.

Even though, on aggregate, European countries want to be role models by aligning rushed deployment and privacy rights, individual countries do not always achieve this goal (Algorithmwatch, 2020). In Norway, for instance, technology-oriented solutionism, specific cultural forms of trust, and the Norwegian dugnaður concept (which refers to collective unpaid and voluntary work), all fostered the rapid deployment of the Norwegian Smittestopp app to fight Covid-19 (Norwegian Institute of Public Health, 2020; Sandvik, 2020: 2). Yet, due to privacy concerns, the Norwegian Data Protection Authority quickly imposed a temporary ban on the Smittestopp contact tracing app (Datatilsynet, 2020).

Rushed adoption of existing technologies

In addition to the rushed deployment of novel technologies, we also witness an expansion in the use of pre-existing technologies. Institutions (such as universities, schools and corporations) were forced to rapidly implement solutions to conduct their daily businesses online. A quick fix that is typically applied in such situations is to obtain consent of students or employees even though public institutions and employers should rely on the legal ground of compliance rather than consent if possible. Institutions rushed to obtain licenses for platforms that otherwise would have undergone more scrutiny from the data protection departments. At a university level, this included software solutions to conduct online teaching, but also online exams such as Proctorio and ExamSoft (Patil and Bromwich, 2020).

The introduction of social distancing has also led to reduced face-to-face interaction between individuals, forcing people to turn to digital alternatives. According to a Gallup poll of US-based adults in April 2020, 25% use social media more frequently since the beginning of the Covid-19 pandemic, 57% use them the same and 7% use them less frequently (10% do not use social media at all) (Ritter, 2020). Zoom has been used for birthday parties (Matyszczyk, 2020) and weddings (Pajer, 2020), while informal get-togethers on apps such as Houseparty are increasingly common (McIntosh, 2020). The forced transition to online socializing raises the question of whether consenting to use social communication platforms can still be considered voluntary during a pandemic.

Rapid adoption of third-party video-conferencing platforms such as Zoom or Skype creates new vulnerabilities in terms of privacy and data protection. Hosts of Zoom calls can see the IP address, location data and device information of participants. Although Zoom made changes to its code in late March 2020 to stop sending data to Facebook (Cox, 2020), privacy concerns about the software continue. One severe social privacy and data security infringement has been Zoombombing (Wakefield, 2020). Zoom has seen much criticism for its privacy policy and security standards during this pandemic (e.g. Leitschuh, 2019; Searls, 2020). This continued pressure forced Zoom to react and thoroughly revise its privacy policy (Zoom, 2020a) (the EDPB as well as the Swiss Federal Data Protection and Information Commissioner (FDPIC) even issued guidance on the safe use of video-conferencing tools as a reaction to this rushed adoption of existing technologies (EDPB, 2020b; FDPIC, 2020b). Zoom claims to have not changed their practices, implying that they have always been compliant. Rather, they claim to have only updated their privacy policy 'to be more clear, explicit, and transparent' (Zoom, 2020b) and to have issued a 90-day feature freeze to address security issues (Zoom, 2020c). In any case, the use of clearer language in their privacy policy improves transparency and strengthens user decision making, according to the principle of informed consent.

The widespread transition to remote work because of Covid-19 has also increased the use of digital surveillance measures in the home (Maalsen and Dowling, 2020). Many professionals currently working from home are now subject to greater surveillance than previously experienced. One example is screen capturing video-services like Sneek, which automatically takes photos of employees through their webcams every five minutes (Holmes, 2020).

Remote work has traditionally raised concerns about the loss of managerial oversight (Sewell and Taskin, 2015), leading to potential worker misbehaviour or slacking. Although recent research has emphasized remote workers' own desire to maintain visibility so they do not feel 'exiled' (Hafermalz, 2020), there are unresolved privacy concerns when workers willingly or unwillingly submit to remote digital surveillance. Although the sales of workplace surveillance tools have increased since the start of the pandemic, privacy concerns about how employers monitor the performance of employees have also grown, raising questions of what form of surveillance is necessary and what forms of surveillance are merely intrusive, such as continuous desktop and webcam sharing (Holmes, 2020; Morrison, 2020).

The regulatory aspects of rushed innovation during the Covid-19 pandemic

Rushed deployment and rushed adoption do not occur in a regulatory vacuum. On the contrary, industry

players and governments are well aware of the comprehensive regulatory frameworks protecting individuals' personal data and privacy. The EU GDPR sets out ample provisions on what must be considered when implementing new processes and adopting new technologies that impinge on individuals' privacy. For instance, private persons processing personal data are required to adopt a privacy-by-design approach (GDPR Article 25), which means that they must consider the privacy implications their new processes and technologies may have on their users and address these implications in their design.

Anyone processing personal data must comply with the general data protection principles (article 5 EU GDPR), particularly the principle of proportionality (which entails the principle of data minimization), the principle of transparency and the principle of purpose limitation. These principles have been discussed in connection with the rushed deployment of new solutions and the rushed adoption of existing technologies. Companies and governments must ensure that only personal data necessary for assessing whether someone may be infected with Covid-19 is processed in their solutions and that access to the collected data was restricted to a strictly need-to-know basis. Moreover, personal information must be deleted once the data is no longer needed and users of these technologies should be transparently informed on how their data is processed. Furthermore, the data processed within these technologies must be adequately protected by technical and organizational safety measures to prevent the accidental and unlawful destruction, loss alteration and the unauthorized disclosure of or access to the collected data (GDPR Article 32). Health data (such as information on flu symptoms or whether someone has tested positive for Covid-19) is particularly strictly regulated, as it is considered as sensitive personal data that requires higher protection than 'regular' personal data (GDPR Article 9).

In general, one relies on the individual's explicit consent to process health data. The rushed and sometimes enforced implementation and use of video-conferencing tools or contact tracing applications raises the question of whether consent to the use of rushed innovations can still be considered voluntary during a pandemic. In any case, whether consent is an adequate tool (Hirsch, 2020; Mayer-Schönberger, 2010) and how it should be implemented digitally (Edenberg and Jones, 2019), have been debated in privacy literature. For those situations, European data protection law requires the data controller to demonstrate that it is possible to refuse or withdraw consent without detriment (GDPR, Recital 42). Thus, the argument can be made that consent currently given online in emergency circumstances might be considered invalid.

Rushed market entrance versus slow regulatory frameworks

From a business perspective, implementing data protection requirements is burdensome and time consuming (Tikkinen-Piri et al., 2018), especially so if there is a pressure to act fast during an emergency. Existing privacy law does not prevent companies from rapidly deploying technologies that are not compliant with data protection law. Companies can conduct initial risk assessments and decide whether it makes more commercial sense to rush deployment, even if the technology is not fully compliant. Companies can choose to act first, and then try to clear-up the privacy-mess later. However, if companies deploy a product that is not compliant with the GDPR, they risk large fines (GDPR Article 83). Even if they are not fined, a supervisory authority may decide to inspect, suspend or completely ban the use of non-compliant technologies (GDPR Article 58).

Introducing products or services to the market that do not demonstrate full legal compliance is not a new phenomenon caused by the Covid-19 pandemic. Medical devices, such as pacemakers, do not always undergo appropriate testing to demonstrate they are safe and effective before entering the market (Van Norman, 2016). In Europe, non-implantable and low-risk devices are self-marked, i.e., the manufacturer itself certifies the compliance and applies for a Conformité Européenne (CE) mark. High-risk devices, however, need to undergo an outside revision process. This involves a notified body which checks compliance with the relevant legislation and issues a CE mark if the device meets the requirements. CE marks across Europe were authorized 'without further controls and no further evaluation' until 2010 when new regulations obliged the approval of devices that are similar to already legally marketed devices (predicate devices) (Jefferys, 2001). The notified-body European system was designed to promote innovation, similar to how the EU GDPR exists purely as a legal framework which favours innovation and allows companies to introduce technologies that process personal data to the market.

However, the goal of the data protection supervisory bodies in Europe is clearly the protection of an individual's privacy interests, which can lead to the supervisory authority stopping, suspending or banning certain technologies if they are not compliant. In this case, the GDPR does provide a certain balance, insofar as companies wanting to introduce new technologies to process personal data may have to conduct a data

protection impact assessment that takes into account 'the nature, scope, context and purposes of the processing' (GDPR Article 35). This especially applies if the envisaged technology entails processing sensitive personal data, such as health data, on a large scale (GDPR Article 35, Para. 3, Letter b).

Governments operate in a tightly regulated environment. In Switzerland, for example, government bodies may process personal data only if a legal basis allows them to do so (Article 17 of the Swiss Federal Act on Data Protection). They cannot take a risk-based approach as companies can. The contact and proximity tracing applications depicted above are a good example of how, although some governments took much longer to deploy these new technologies, they worked together with privacy scholars and data protection authorities to ensure compliance with privacy laws. The Norwegian example shows that if you go to market with a non-compliant tool, your product may be banned or its use may be suspended until it is compliant which is even more detrimental than just slowing down the process to be fully compliant.

The difference between the rushed deployment and adoption of medical devices and privacy-harvesting digital technologies is that 'interference with data protection rights does not depend on whether there has been any harm or inconvenience to an individual' (Kuner et al., 2015). The example of Zoom shows that it is possible to adopt existing technologies and scale their use in a very short time, even though they are very privacy unfriendly, and then the company can clean their 'privacy-mess' up retrospectively.

Given that some of these technologies process information that may have an ulterior impact on the population's health, however, such an interference could be more salient. At least, that is how some data protection authorities have interpreted it, halting Covid-19 solutions due to data processing concerns (Datatilsynet, 2020). The state of force majeure and the demand for a hurried response to ensure the safety of the population's life and health allowed the deployment of 'a highly invasive and technically unfinished app on their population' that did not go through a tendering process or appropriate risk assessments (Sandvik, 2020). Indeed, after a thorough balance-of-interest exercise between health benefits and adverse privacy impacts, the Norwegian Data Protection Authority imposed a temporary ban on the Smittestopp contact tracing app (Datatilsynet, 2020).

Emergency laws and exemptions to foster rushed innovation

What are companies and governments supposed to do in emergencies when the protection of public health is of utmost importance, and individuals are willing to risk their privacy for the greater good? The GDPR provides a semi-useful solution. As it stands, processing health data is lawful if it is

> necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health [...] on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject.

Therefore, based on local law, it may be permitted to process health data without consent and even without complying with all the requirements set out in the GDPR if local emergency law permits.

In light of this, governmental authorities have created guidelines to tackle data analysis practices during the Covid-19 pandemic, arguing that privacy and health protection can go hand in hand. The Committee of the Global Privacy Assembly (GPA) issued a guiding statement in March 2020, supporting governments and organizations to share personal information to fight the spread of the virus. The GPA (2020) states:

> We are confident that data protection requirements will not stop the critical sharing of information to support efforts to tackle this global pandemic. The universal data protection principles in all our laws will enable the use of data in the public interest and still provide the protections the public expects. Data protection authorities stand ready to help facilitate swift and safe data sharing to fight COVID-19.

This GPA guidance is in line with approaches already taken by national data protection authorities, such as the European Data Protection Board (EDPB), the CNIL in France, the ICO in the UK and the FDPIC in Switzerland. In Europe, the measures taken under applicable law either rely on an overriding public or private interest or a statutory duty to implement the actions needed to contain and fight the spread of such a pandemic as long as the general data protection principles described above are complied with as far as the situation allows (EDPB, 2020a; FDPIC, 2020a; CNIL, 2020; ICO, 2020; PCPD 2020). However, individual governments can decide what measures they deem necessary to fight Covid-19 and how they can justify these measures. These can be either by public interest, such as the protection of public health, statutory law, such as the Swiss Epidemics Act or the UK Regulation 3(4), or even by calling a state of emergency. Some countries may even use emergency measures to overturn the rule

of law to fight the pandemic, such as witnessed earlier this year in Hungary (Rohac, 2020).

On 8 April 2020, the European Commission adopted the *Communication from the Commission Guidance on Apps supporting the fight against Covid 19 pandemic in relation to data protection 2020/C 124 I/01* (European Commission, 2020), establishing non-binding requirements to ensure app developers comply with EU privacy and personal data protection legislation (GDPR and e-Privacy Directive). Among these requirements, the European Commission stresses that apps should have an explicit and precise processing purpose; ensure data security and accuracy; implement strict data disclosure, access and storage limitation; and use the data minimization principle.

As a legitimate basis for data processing, the European Commission reminds that GDPR Article 5 e-Privacy Directive requires the consent of the user to store or gain access to information already stored on the user's device, unless the storage is necessary for the app, and the user has explicitly requested it. GDPR Article 6(1)(e) also allows the processing of personal data to perform a task of public interest. The general privacy principles of purpose limitation, proportionality and transparency do not prohibit the surveillance measures currently taken by governments or organizations, but rather ensure the correct handling of the data once processed under the current circumstances (GPA, 2020).

While there seems to be some consensus on allowing rushed innovation in emergency situations and the adoption of emergency law may even let the processing of personal data even in non-compliance with applicable data protection law, at the same time, neither governments nor industry players took this direction (maybe because they were too afraid of the fines under the EU GDPR). This illustrates that there is no proper or comprehensive exception in privacy law itself that would explicitly allow the rushed deployment of new solutions or the rushed adoption of existing technologies which do not fully comply with the general data protection principles, as there is, for example, with regard to processing personal data for research and scientific purposes. The existing law was not tailored to handle emergencies, and this may be due to the governmental powers in such situations that can be used to override regulatory frameworks to rush innovation in breach of data protection law for the greater good if it came to it.

What all our examples show is that, in reality, privacy becomes the core value to be protected regardless of the public health benefits that privacy-invasive technologies may bring about. What we need if we want more legal certainty may be something more clear than the public health exemption which explicitly allows rushed innovation that is not compliant with privacy laws in situations of emergency. A solution could be an exemption similar to the GDPR research exemption, which states that data processing for research purposes is not considered incompatible with the initial purpose as long as safeguards are put in place (Articles 5 (1) b and 89).

While this mainly alleviates the burden regarding the legal basis for data processing, it does not help shorten the data protection impact assessment (DPIA), which might have been one of the main reasons for slower deployment. While the GDPR already allows for weighing of different interests, DPIA provisions would need to explicitly allow for interests other than privacy to be considered. Similar to the research exemption, the reasoning would also be to benefit the greater good. If higher-weighted interests, such as public or individual health, could allow for lower burden of proof, this could provide the much needed legal certainty for states and corporations in such emergency situations, where decisions have to be made based on scarce and unclear information. Such a process could enable actors to anticipate and mitigate data protection risks in emergency situations to the population, including vulnerable groups.

Conclusion: Lessons learned and steps ahead

The global spread of Covid-19 shows that, in an emergency, governments are willing and permitted to implement extraordinary measures to combat such a pandemic even if these measures directly affect the rights and freedoms of individuals. On a personal level, citizens seem to be shifting towards protecting public health over privacy across different contexts. However, 'when choosing between alternatives, we should ask ourselves not only how to overcome the immediate threat, but also what kind of world we will inhabit once the storm passes' (Harari, 2020).

In this sense, a first lesson learned is that the urgency of states of emergency is not always compelling enough to suppress one right against another in a balance-of-interest exercise. On the contrary, fundamental rights need to be protected equally. This pandemic, and the reactions of public authorities as well as society, show that rushed measures implemented during a state of emergency are accepted only to a certain extent, and only if they are in line with other fundamental rights. This does not hinder the implementation of measures that interfere with the privacy of citizens, but it requires governments and the industry to be mindful and compliant with existing regulations, beyond raising awareness to society. Employers, for instance, are required to

assist governments with the implementation of such measures. On the other hand, they have a duty of care to protect their employees' health, thus permitting employees to work from home and requiring employees to report symptoms connected to Covid-19. Moreover, employers must also ensure their operative business, which is why some have resorted to far-reaching employee surveillance. In this sense, a further key lesson learned is that designing privacy-friendly solutions may dissipate the concerns that the pandemic could be exploited as an opportunity to normalize governmental surveillance to a certain degree.

The banning of different applications in the fight against Covid-19, due to privacy concerns, poses the additional question of whether these ex-post temporary measures are a call out in favour of privacy or whether they elucidate the weakness of data protection regulation effectiveness. Banning COVID-related applications may be an opportunity to stress the importance of enforcing data protection principles, even in emergency states. However, it also illustrates the potential waste of resources that non-compliant solutions may entail. What remains unclear is what happens to the user's personal information and the data protection issues arising from the use and deployment of such solutions.

For users, one lesson learned is that they should inform themselves about the privacy risks involved with newly deployed technologies such as contact tracing apps, rather than rushing to adopt them in the interest of the public good. While scholarship has warned against putting the onus of responsibility squarely on the individual when it comes to privacy (Obar, 2015), users still have power to vote with their feet, particularly for technologies that rely on network effects such as contact tracing apps. Of course, voluntary adoption decisions are not always possible, as governments and employers either aggressively nudge (Sandvik, 2020) or even force citizens to rapidly adopt problematic solutions in terms of privacy (Algorithmwatch, 2020, where the Slovenia country report by Lenart Kučić describes the 'looming spectre of a mandatory tracking app'). Here, a critical public sphere is key that brings privacy and tech scandals to the surface, holding those responsible accountable through reputational pressure (Kolkman, 2020). Rushed adoption, and technology-infused rush more generally, can be counteracted on the user level by slow computing (Kitchin and Fraser, 2020), where users seek out more balanced digital lives through conscious initiatives and reflection.

From a research perspective, the investigation of data technologies within the pandemic is only at the beginning. Research has started to reflect on the privacy implications of the Covid-19 pandemic (Vitak and Zimmer, 2020), especially regarding the spatial dimensions and location-based data (Frith and Saker, 2020; Poom et al., 2020). It is not surprising that spatial aspects have been prioritized over temporal ones, given the data being collected within many applications to mitigate the pandemic and the strong spatial considerations that come with the pandemic (e.g. quarantine and social distancing as key spatial strategies). However, such data is often also temporal and we have argued that scholars should pay close attention to the temporal dynamics of the pandemic when it comes to privacy. For instance, to what extent can we use privacy assessments before the deployment of technological solutions to anticipate and help mitigate adverse privacy implications? More conceptual analysis and synthesis are needed to connect the first steps made in this paper to established theories of time and technology (Rosa, 2013; Wajcman, 2015) and newer work (Kitchin and Fraser, 2020).

Rushed innovation in disaster capitalism (Klein, 2007) should be investigated empirically. Case studies, such as the one discussed by Sandvik (2020), offer a fruitful approach to analyze the deployment of new solutions. We encourage qualitative researchers to document and critically investigate the temporalities of technology projects relating to the pandemic. On the adoption side, case studies could accompany the decision-making processes within organizations and public institutions that lead to rushed adoption, spotlighting privacy implications for those affected. Recent examples that ask for critical inquiry are the introduction of proctoring software at universities (Patil and Bromwich, 2020), the application of grading algorithms for A levels in UK schools (Hern, 2020; Kolkman, 2020), and the increased use of workplace surveillance software such as Hubstaff (Jones, 2020). These examples also show the intertwinement of privacy risks with intersectional concerns for rushed innovation. Those more vulnerable and marginalized in society face disproportionate privacy repercussions and more general risks from Big Data in the wake of the pandemic (Milan and Treré, 2020).

Digital inequalities research has looked into digital communication changes that come with the pandemic and how these changes are unequally distributed, favouring individuals with advanced Internet skills (Nguyen et al., 2020). Future research should study the disparate intersectional implications of rushed innovation. Quantitative surveys could be combined with qualitative and ethnographic studies with those at the margins (Marwick and boyd, 2018), giving distinct voice to their concerns. Action research from a social justice-based perspective is particularly promising, as it involves marginalized communities and emphasizes practical change through design initiatives

(Costanza-Chock, 2020). Outside of organizations and institutions, rushed innovation can be investigated with a variety of user-oriented methods, including digital methods such as walkthroughs (Light et al., 2018), glitch studies analyses (Menkman, 2011), and sentiment analysis, social network analysis, or topic models of social media coverage (Sloan and Quan-Haase, 2017).

Pandemics and other world catastrophes push for immediate responses. Still, these responses will have many consequences for society in the immediate and long run that require a thorough understanding of how responsible rushed innovation can be. Greater effort in incorporating privacy considerations beforehand in the design of digital solutions is very much needed, as afterthought privacy reflections risk exposing the health of citizens, wasting public resources and worsen the consequences that the state of emergency already has for society.

Acknowledgements

We would like to thank the editorial team of *Big Data & Society* as well as three anonymous peer reviewers for a constructive and helpful peer review process.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Gemma Newlands and Christoph Lutz received funding from the Research Council of Norway under grant agreement 275347 'Future Ways of Working in the Digital Economy'. Eduard Fosch Villaronga received funding from the LEaDing Fellows Marie Curie COFUND fellowship, a project funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 707404. Aurelia Tamò-Larrieux received funding from the Digital Society Initiative fellowship (University of Zurich, Switzerland) and the International Postdoctoral Fellowship grant (University of St. Gallen, Switzerland; project number 1031564).

ORCID iD

Christoph Lutz https://orcid.org/0000-0003-4389-6006

References

Algorithmwatch (2020) ADM systems in the COVID-19 pandemic: A European perspective. Algorithmwatch, 1 September 2020. Available at: https://algorithmwatch.org/en/project/automating-society-2020-covid19/ (accessed 3 September 2020).

Andrejevic M and Gates K (2014) Big data surveillance. *Surveillance & Society* 14(2): 185–196.

Balsari S, Buckee C and Khanna T (2020) Which Covid-19 data can you trust? *Harvard Business Review*, 8 May 2020. Available at: https://hbr.org/2020/05/which-covid-19-data-can-you-trust (accessed 1 June 2020).

Bigo D (2006) Security, exception, ban and surveillance. In: Lyon D (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan, pp.46–68.

Bryan K, Lemus J and Marshall G (2020) Innovation during a crisis: Evidence from Covid-19. *SSRN Electronic Journal* (29 April 2020) Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3587973 (accessed 3 September 2020).

Buckee C (2020) Improving epidemic surveillance and response: Big data is dead, long live big data. *The Lancet Digital Health* 2(5): e218–e220.

Calhoun C (2010) The idea of emergency: Humanitarian action and global (dis)order. In: Fassin D and Pandolfi M (eds) *Contemporary States of Emergency: The Politics of Military and Humanitarian Interventions*. New York: Zone Books, pp.29–58.

Callaway E (2020) Russia's fast-track coronavirus vaccine draws outrage over safety. *Nature* 584: 334–335.

Carillo JE (2005) Industry clockspeed and the pace of new product development. *Production and Operations Management* 14(2): 125–141.

Cheung S (2020) Disambiguating the benefits and risks from public health data in the digital economy. *Big Data & Society* 7(1): 1–15.

Cho H, Ippolito D and Yu YW (2020) Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv* preprint arXiv:2003.11511. Available at: https://arxiv.org/abs/2003.11511 (accessed 4 April 2020).

Commission nationale de l'informatique et des libertés (CNIL) (2020) Coronavirus (Covid-19): les rappels de la CNIL sur la collecte de données personnelles. Available at: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles (accessed 29 March 2020).

Corriere Della Sera (2020) Coronavirus, Regione: In Lombardia 2 mila contagiati in più. Non uscite, controlli anche su celle telefoniche. Available at: https://milano.corriere.it/notizie/cronaca/20_marzo_17/coronavirus-gallera-in-lombardia-1640-decessi-16620-positivi-e3875744-686d-11ea-9725-c592292e4a85.shtml (accessed 5 April 2020).

Costanza-Chock S (2020) *Design Justice: Community-Led Practices to Build the World We Need*. Cambridge: MIT Press.

Cox J (2020) Zoom removes code that sends data to Facebook. *Vice*, 27 March. Available at: https://www.vice.com/en/article/z3b745/zoom-removes-code-that-sends-data-to-facebook (accessed 6 April 2020).

Dalg P (2020) RKI bekommt Handydaten von Deutscher Telekom. *Der Tagesspiegel*, 18 March. Available at: https://www.tagesspiegel.de/wissen/wie-breitet-sich-das-coronavirus-aus-rki-bekommt-handydaten-von-deutscher-telekom/25655144.html (accessed 5 April 2020).

Datatilsynet (2020) The Norwegian Data Protection Authority has imposed a temporary ban on Smittestopp contact tracing mobile application. Available at: https://www.datatilsynet.no/en/news/2020/the-norwegian-data-protection-authority-has-imposed-a-temporary-ban-on-smittestopp-contact-tracing-mobile-application/ (accessed 30 September 2020).

Dubov A and Shoptaw S (2020) The value and ethics of using technology to contain the COVID-19 epidemic. *The American Journal of Bioethics* 20(7): W7–W11.

Edenberg E and Jones ML (2019) Analyzing the legal roots and moral core of digital consent. *New Media & Society* 21(8): 1804–1823.

Eisenhardt K and Martin J (2000) Dynamic capabilities: What are they? *Strategic Management Journal* 21(10–11): 1105–1121.

Etherington D and Lomas N (2020) Apple and Google update joint coronavirus tracing tech to improve user privacy and developer flexibility. TechCrunch, 24 April 2020. Available at: https://techcrunch.com/2020/04/24/apple-and-google-update-joint-coronavirus-tracing-tech-to-improve-user-privacy-and-developer-flexibility/

European Commission (2020) Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0417(08) (accessed 9 June 2020).

European Data Protection Board, EDPB (2020a) Statement on the processing of personal data in the context of the COVID-19 outbreak. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (accessed 3 April 2020).

European Data Protection Board, EDPB (2020b) Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices.pdf (accessed 3 October 2020).

Federal Data Protection and Information Commissioner, FDPIC (2020a) Updates - Datenschutzrechtlicher Rahmen bei der Eindämmung des Coronavirus: Zugang des BAG zu visualisierten Daten der Swisscom datenschutzrechtlich erlaubt. Available at: https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#1781027723 (accessed 13 April 2020).

Federal Data Protection and Information Commissioner, FDPIC (2020b) Measures for the safe use of audio and video conferencing systems. Available at: https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-1113581112 (accessed 3 October 2020).

Ferretti L, Wymant C, Kendall M, et al. (2020) Quantifying SARS-Cov-2 transmission suggests epidemic control with digital contact tracing. *Science* 368(6491): eabb6936.

French M and Monahan T (2020) Disease surveillance: How might surveillance studies address Covid-19? *Surveillance & Society* 18(1): 1–11.

French M, Mykhalovskiy E and Lamothe C (2018) Epidemics, pandemics and outbreaks. In: Treviño J (ed.) *The Cambridge Handbook of Social Problems*. Cambridge: Cambridge University Press, pp.59–77.

Frith J and Saker M (2020) It is all about location: Smartphones and tracking the spread of COVID-19. *Social Media + Society* 6(3): 1–14.

Gasser U (2016) Recoding privacy law: Reflections on the future relationship among law, technology, and privacy. *Harvard Law Review Forum – Law, Privacy & Technology Commentary Series* 130(2): 61–70.

Gasser U, Ienca M, Scheibner J, et al. (2020) Digital tools against COVID-19: Framing the ethical challenges and how to address them. arXiv preprint arXiv:2004.10236. Available at: https://arxiv.org/abs/2004.10236 (accessed 9 June 2020).

Ghosh S (2020) Privacy activists fear the UK might spy on its own citizens to tackle COVID-19. Here's what we know. *Business Insider*. Available at: https://www.businessinsider.com/explainer-coronavirus-uk-phone-tracking-2020-3?IR=T (accessed 5 April 2020).

Global Privacy Assembly (GPA) (2020) Statement by the GDP Executive Committee on the Coronavirus (COVID-19) pandemic. Available at: https://cnpd.public.lu/en/actualites/international/2020/03/gpa-corona.html (accessed 29 March 2020)

Griffin A, Langerak F and Eling K (2019) The evolution, status and research agenda for the future of research in NPD cycle time. *Journal of Product Innovation Management* 36(3): 263–280.

Ha YP, Tesfalul MA, Littman-Quinn R, et al. (2016) Evaluation of mobile health approach to tuberculosis contact tracing in Botswana. *Journal of Health Communication* 21(10): 1115–1121.

Hafermalz E (2020) Out of the panopticon and into exile: Visibility and control in distributed new culture organizations. *Organization Studies*. Epub ahead of print 14 April 2020. DOI: 10.1177/0170840620909962.

Harari YN (2020) The world after coronavirus. *Financial Times*, 19 March. Available at: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (accessed 4 April 2020).

Harris M, Bhatti Y, Buckley J, et al. (2020) Fast and frugal innovations in response to the Covid-19 pandemic. *Nature Medicine* 26: 814–821.

Hermosilla M (2020) Rushed innovation: Evidence from drug licensing. *Management Science* Epub ahead of print 8 April 2020. DOI: 10.1287/mnsc.2019.3530.

Hern A (2020) Ofqual's A-level algorithm: Why did it fail to make the grade? *The Guardian*, 21 August. Available at: https://www.theguardian.com/education/2020/aug/21/ofqual-exams-algorithm-why-did-it-fail-make-grade-a-levels (accessed 2 October 2020).

Hirsch DD (2020) From individual control to social protection: New paradigms for privacy law in the age of predictive analytics. *Maryland Law Review* 79(2): 439–505.

Holmes A (2020) Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working - and the service is seeing a rapid

expansion since the coronavirus outbreak. *Business Insider Australia*, 24 March. Available at: https://www.businessinsider.com.au/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3 (accessed 6 April 2020).

Information Commissioner's Office (ICO) (2020) Data protection and coronavirus information hub. Available at: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/ (accessed 13 April 2020).

Jefferys DB (2001) The regulation of medical devices and the role of the Medical Devices Agency. *British Journal of Clinical Pharmacology* 52(3): 229–235.

Jones L (2020) 'I monitor my staff with software that takes screenshots'. *BBC*, 29 September 2020. Available at: https://www.bbc.com/news/business-54289152 (accessed 2 October 2020).

Kessler E and Chakrabarti A (1996) Innovation speed: A conceptual model of context, antecedents and outcomes. *The Academy of Management Review* 21(4): 1143–1191.

Kitchin R (2020) Using digital technologies to tackle the spread of the coronavirus: Panacea or folly? The Programmable City Working Paper 44. Available at: http://progcity.maynoothuniversity.ie/wp-content/uploads/2020/04/Digital-tech-spread-of-coronavirus-Rob-Kitchin-PC-WP44.pdf (accessed 9 June 2020).

Kitchin R and Fraser A (2020) *Slow Computing: Why We Need Balanced Digital Lives*. Bristol: Bristol University Press.

Klein N (2007) *The Shock Doctrine*. London: Penguin.

Kolkman D (2020) "F**k the algorithm"? What the world can learn from the UK's A-level grading fiasco. *LSE Impact Blog*, 26 August 2020. Available at: https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/ (accessed 2 October 2020).

Kuner C, Cate FH, Millard C, et al. (2015) Risk management in data protection. *International Data Privacy Law* 5(2): 95–98.

Lai S and Flensburg S (2020) A proxy for privacy uncovering the surveillance ecology of mobile apps. *Big Data & Society* 7(2): 1–20.

Leitschuh J (2019) Zoom zero day: 4+ Million webcams & maybe an RCE? Just get them to visit your website. *Medium Infosec Write-Ups*. Available at: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5 (accessed 3 April 2020).

Leslie D (2020) Tackling Covid-19 through responsible AI innovation: Five steps in the right direction. *SSRN Electronic Journal,* 14 May 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3652970 (accessed 3 September 2020).

Light B, Burgess J and Duguay S (2018) The walkthrough method: An approach to the study of apps. *New Media & Society* 20(3): 881–900.

Liu R and Kim M (2020) Sinovac's coronavirus vaccine candidate approved for emergency use in China – Source. *Reuters*, 28 August 2020. Available at: https://www.reuters.com/article/us-health-coronavirus-china-vaccines/sinovacs-coronavirus-vaccine-candidate-approved-for-emergency-use-in-china-source-idUSKBN25O0Z3 (accessed 3 September 2020).

Liu R and Woo R (2020) CanSino's COVID-19 vaccine candidate approved for military use in China. *Reuters*, 29 June 2020. Available at: https://www.reuters.com/article/us-health-coronavirus-china-vaccine/cansinos-covid-19-vaccine-candidate-approved-for-military-use-in-china-idUSKBN2400DZ#:~:text=China's%20Central%20Military%20Commission%20approved,of%20Military%20Science%20(AMS) (accessed 3 September 2020).

Lyon D (2003) *Surveillance after September 11*. Cambridge: Polity.

Maalsen S and Dowling R (2020) Covid-19 and the accelerating smart home. *Big Data & Society* 7(2): 1–5.

Marwick AE and boyd d (2018) Understanding privacy at the margins. *International Journal of Communication* 12: 1157–1165.

McIntosh F (2020) Zoom fatigue? Try Houseparty. *The New Yorker*, 1 June 2020. Available at: https://www.newyorker.com/magazine/2020/06/08/zoom-fatigue-try-houseparty (accessed 3 September 2020).

Madianou M (2020) A second-order disaster? Digital technologies during the COVID-19 pandemic. *Social Media + Society* 6(3): 1–5.

Matyszczyk C (2020) I went to a 50-person Zoom party and I may never recover. *ZDNet*, 17 May. Available at: https://www.zdnet.com/article/i-went-to-a-50-person-zoom-party-and-i-may-never-recover/ (accessed 3 September 2020).

Mayer-Schönberger V (2010) Beyond privacy, beyond rights - Toward a systems theory of information governance. *California Law Review* 98: 1853–1885.

Menkman R (2011) Glitch studies manifesto. *Video vortex reader II: Moving images beyond YouTube*, 336–347. Available at: https://pdfs.semanticscholar.org/0732/56f0c90a712365890f379f7dc55bd1377f3e.pdf (accessed 3 September 2020).

Milan S and Treré E (2020) The rise of the data poor: The COVID-19 pandemic seen from the margins. *Social Media + Society* 6(3): 1–5.

Milne R and Costa A (2020) Disruption and dislocation in post-Covid futures for digital health. *Big Data & Society* 7(2): 1–5.

Morley J, Cowls J, Taddeo M, et al. (2020) Ethical guidelines for COVID-19 tracing apps. *Nature* 582: 29–31.

Morrison S (2020) Just because you're working from home doesn't mean your boss isn't watching you. *Vox*, 2 April. Available at: https://www.vox.com/recode/2020/4/2/21195584/coronavirus-remote-work-from-home-employee-monitoring (accessed 14 April 2020).

Nguyen MH, Gruber J, Fuchs J, et al. (2020) Changes in digital communication during the COVID-19 global pandemic: Implications for digital inequality and future research. *Social Media + Society* 6(3): 1–6.

Norwegian Institute of Public Health (2020) Together we can fight coronavirus - Download the Smittestopp app. helsenorge.no, 28 (April 2020) Available at: https://helsenorge.no/coronavirus/smittestopp (accessed 3 November 2020, redirected to https://www.helsenorge.no/en/coronavirus/).

Obar JA (2015) Big Data and *The Phantom Public*: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society* 2(2): 1–16.

Orlikowski WJ and Yates J (2002) It's about time: Temporal structuring in organizations. *Organization Science* 13(6): 684–700.

Pajer N (2020) A virtual DJ, a drone, and an all-out zoom wedding. *Wired*, 21 May 2020. Available at: https://www.wired.com/story/virtual-dj-drone-all-out-zoom-wedding/ (accessed 3 September 2020).

Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT (2020) Available at: https://www.pepp-pt.org (accessed 5 April 2020; website down as of 3 November 2020).

Parker MJ, Fraser C, Abeler-Dörner L, et al. (2020) Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics* 46(7): 427–430.

Patil A and Bromwich JE (2020) How it feels when software watches you take tests. *New York Times*, 29 September. Available at: https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html (accessed 2 October 2020).

Privacy Commissioner for Personal Data (PCPD) (2020) The use of information on social media for tracking potential carriers of COVID-19. Available at: https://www.pcpd.org.hk/english/media/media_statements/press_20200226.html (accessed 29 March 2020).

Polish Government (2020) Aplikacja "Kwarantanna domowa" – ruszył proces jej udostępniania. Available at: https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa–ruszyl-proces-jej-udostepniania (accessed 5 April 2020).

Poom A, Järv O, Zook M, et al. (2020) Covid-19 is spatial: Ensuring that mobile Big Data is used for social good. *Big Data & Society* 7(2): 1–7.

Raymond S (1999) *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol: O'Reilly Media.

Ries E (2011) *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses*. New York: Crown Press.

Ritter Z (2020) Americans use social media for COVID-19 info, connection. *Gallup*. Available at: https://news.gallup.com/poll/311360/americans-social-media-covid-information-connection.aspx (accessed 4 October 2020).

Rohac D (2020) Hungary's prime minister is using the virus to make an authoritarian power grab. The Washington Post, 25 March. Available at: https://www.washingtonpost.com/opinions/2020/03/25/hungarys-prime-minister-is-using-virus-make-an-authoritarian-power-grab/ (accessed 13 April 2020).

Rosa H (2013) *Social Acceleration: A New Theory of Modernity*. New York: Columbia University Press.

Sacks JA, Zehe E, Redick C, et al. (2015) Introduction of mobile health tools to support Ebola surveillance and contact tracing in Guinea. *Global Health, Science and Practice* 3(4): 646–659.

Sandvik KB (2020) "Smittestopp": If you want your freedom back, download now. *Big Data & Society* 7(2): 1–11.

Schneier B (2015) *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W W Norton and Company.

Searls D (2020) Zoom needs to clean up its privacy act. *Doc Searls Weblog*. Available at: https://blogs.harvard.edu/doc/2020/03/27/zoom/ (accessed 3 April 2020).

Sewell G and Taskin L (2015) Out of sight, out of mind in a new world of work? Autonomy, control and spatiotemporal scaling in telework. *Organization Studies* 36(11): 1507–1529.

Sloan L and Quan-Haase A (eds) (2017) *The SAGE Handbook of Social Media Research Methods*. London: Sage.

Steiger M (2020) Standortdaten gegen COVID-19: Wo bleibt die Transparenz? *Steiger Legal*. Available at: https://steigerlegal.ch/2020/03/29/bag-swisscom-covid19-transparenz/ (accessed 13 April 2020).

Taneja H (2019) The era of "move fast and break things" is over. *Harvard Business Review*, 21 January 2019. Available at: https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over (accessed 3 September 2020).

Taylor L (2020) The price of certainty: How the politics of pandemic data demand an ethics of care. *Big Data & Society* 7(2): 1–7.

Tikkinen-Piri C, Rohunen A and Markkula J (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review* 34(1): 134–153.

Toh A and Brown D (2020) How digital contact tracing for COVID-19 could worsen inequality. *Human Rights Watch*. Available at: https://www.hrw.org/news/2020/06/04/how-digital-contact-tracing-covid-19-could-worsen-inequality (accessed 12 June 2020).

Topak Ö (2017) The making of a totalitarian surveillance machine: Surveillance in Turkey under AKP rule. *Surveillance & Society* 15(3/4): 535–542.

Tromble R and McGregor SC (2019) You break it, you buy it: The naiveté of social engineering in tech–and how to fix it. *Political Communication* 36(2): 324–332.

Troncoso C, Payer M, Hubaux JP, et al. (2020) Decentralized privacy-preserving proximity tracing. *GitHub*. Available at: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf (accessed 5 April 2020).

Vallee M (2020) Doing nothing does something: Embodiment and data in the Covid-19 pandemic. *Big Data & Society* 7(1): 1–12.

Van Norman GA (2016) Drugs and devices: Comparison of European and US approval processes. *JACC: Basic to Translational Science* 1(5): 399–412.

Vitak J and Zimmer M (2020) More than just privacy: Using contextual integrity to evaluate the long-term risks from Covid-19 surveillance technologies. *Social Media + Society* 6(3): 1–4.

Wajcman J (2015) *Pressed for Time: The Acceleration of Life in Digital Capitalism*. Chicago: University of Chicago Press.

Wajcman J (2019) How silicon valley sets time. *New Media & Society* 21(6): 1272–1289.

Wakefield J (2020) Coronavirus: Racist 'zoombombing' at virtual synagogue. *BBC*. Available at: https://www.bbc.com/news/technology-52105209 (accessed 5 October 2020).

Waterson J (2020) Boris Johnson urges top UK tech firms to join coronavirus fight. *The Guardian*. Available at: https://www.theguardian.com/business/2020/mar/13/johnson-urges-top-uk-tech-firms-to-join-coronavirus-fight (accessed 5 April 2020).

Wyss W (2020) Analysis of mobile phone data during the COVID-19 pandemic in Switzerland. *Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=bd8a18f3-1d69-4331-ac5e-0d591df59551 (accessed 5 April 2020).

York JC and McSherry C (2020) Automated moderation must be temporary, transparent and easily appealable. *Electronic Frontier Foundation*, 2 April 2020.

Zoom (2020a) Privacy Policy. *Zoom Blog*. Available at: https://zoom.us/privacy (accessed 3 April 2020).

Zoom (2020b) Zoom's Privacy Policy. *Zoom Blog*. Available at: https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/ (accessed 3 April 2020).

Zoom (2020c) A message to our users. *Zoom Blog*. Available at: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ (accessed 3 April 2020).