CHAPTER 1

Digital Health: Data Traps at Our Fingertips

Introduction

'There's an app for that!': A catchy internet phrase of the mid 2000s, initiated and subsequently trademarked by Apple, captures what has become an everyday reality for most digital economies. With the widespread use of smart phones, we are increasingly reliant on apps that are either pre-loaded or can be voluntarily/casually and mandatorily/professionally downloaded, to manage all areas of our consumer, work, political and personal lives. The sheer volume, range, speed and breadth of the different types of apps available today demonstrates that an all-encompassing appisation is now an inevitable part of contemporary digital life (Gardner and Davis 2013; Miller and Matviyenko 2014; Morris and Murray 2018).

Apps, and their social consequences, will be discussed throughout our book. In this chapter, we start with the appisation of health– or 'mHealth/mobile Health' as the process is more commonly described in medical circles. At present, countless apps are developed and offered to individual smartphone users to manage 'healthy lifestyles' or to support specific medical and health conditions; the apps are also extensively integrated into both public and private health services provisions (Lupton 2014; van Dijck and Poell 2016). However, the invisible yet detrimental 'by-products' of health appisation, such as infringements on privacy, data monetisation and long-term digital profiling, are rarely understood by the medical practitioners and health service providers who recommend the apps. Nor are these by-products always clear to the users, who are lured by the speed and convenience of 'on demand healthcare', usually advertised as an 'affordable and accessible service at one's fingertips', to use the words of Babylon Health, one of the leading health apps (Babylon

How to cite this book chapter:
Kuntsman, A. and Miyake, E. 2022. *Paradoxes of Digital Disengagement: In Search of the Opt-Out Button*. Pp. 21–39. London: University of Westminster Press. DOI: https://doi.org/10.16997/book61.b. License: CC-BY-NC-ND 4.0

2016). Health appisation is thus presented as an unquestionably positive process, devoid of dangers and beneficial to all. It is a celebratory framing which both conceals and supports the apps' data economy of 'surveillance capitalism' (Cinnamon 2017; Lehtiniemi 2017; Silverman 2017; Zuboff 2019) that relies on users' willing but often unknowing participation and the continuous personal 'contribution' of their data.

While health appisation may indeed have revolutionised some aspects of health care, its broader, and often perturbing socio-political effects, are yet to be explored in the academic domain of digital health. For example, Deborah Lupton argues that most studies on health apps to date come from medical or public health literature, which focuses primarily on an instrumental approach to apps' effectiveness or medical validity (Lupton 2014). What is yet to be interrogated are '[t]he wider social, cultural, and political roles played by health and medical apps as part of contemporary healthcare and public health practice'– a task she sets out for 'critical digital health studies' (2014, 607). This chapter takes Lupton's call further by examining the appisation of health through the perspective of digital disengagement. Rather than only addressing the way health apps turn biodata into profit through surveillance capitalism dressed as 'smart' and effective healthcare, we turn our attention to how the apps navigate – and often block or limit – the possibility of opting out of health datafication. In this chapter, we approach health apps not just as what Lupton (2014) calls 'sociocultural artefacts', but as *socio-cultural data traps*, elaborate and sophisticated in their technologies of incorporation and engagement, yet incredibly scarce in social affordances and technical mechanisms for letting their 'data subjects' go or allowing them to remove themselves from the database. The central concern in this chapter, therefore, is how opt-out as a legal, social and technical possibility, and as a citizen and user right, plays out within the sphere of digital health. Questions of digital disengagement and opting out of digital health are of particular urgency because of the intimate relationship between health and personal data, which the process of appisation transforms. Before the Covid-19 pandemic, the health field had already been radically transformed by digital technologies. And now this transformation is being further accelerated by the global public health crisis.

We begin our discussion by looking at the current legal and political landscape of digital health and opt-out in the UK, where the publicly funded national health system co-exists with health apps, which are independently developed and mostly privately owned. We then move on to closely examining some health apps' Terms and Conditions, Privacy Policies and app interfaces from the perspective of how opt-out is presented as a legal, technical and practical option. Finally, we discuss the National Health Service (NHS) Covid-19 contact tracing app, its introduction in the UK in autumn 2020, and the way it impacted debates around appisation, public health and personal data. We conclude the chapter by making a differentiation between individual and collective opt-outs. While the former is made possible by legal frameworks, such as the

European General Data Protection Regulation (GDPR), and by some of the apps' policies, design and interface, we will argue that individual opt-outs have no meaning without considering collective and structural forces such as the data economy, or population surveillance. It is then that we introduce an argument that first emerged in our analysis of digital health but continues through the rest of the book: it is imperative that we shift from individual digital rights to collective digital justice.

NHS Digital and the App Library: What Is One Opting Out Of?

As in many other digital economies, the health sector in the UK increasingly expects patients to manage their own health and wellbeing through apps. Health apps are widely offered by private companies and have also been adopted by the public sector and the NHS, especially NHS Digital, 'the national information and technology partner to the health and care system' (NHS Digital n.d.). The incorporation of apps into NHS Digital is the latest development in a longer tradition of online and over-the-phone patient support, designed to reduce GP and hospital workload. It should thus be understood within a broader context of continuous budget cuts in the free national healthcare system, leading to diminishing resources for face-to-face and on-site patient support. Some of this support is replaced with automated services like online symptom checkers, as well as 'social prescribing' where patients are referred to social activities rather than medical treatment, to manage their health, in partnership with patient groups and the voluntary sector (Culture Health and Wellbeing Alliance n.d.). At the same time, this is also part of a general move towards 'self-responsibilisation' for one's health (Juhila, Raitakari and Hall 2017; Lucas 2015; Øvretveit 2015; Morton et al. 2017) within the wider Euro-American neoliberal context, that exists across countries with public, semi-private and private health care.

In 2018, two major legal developments took place which are pivotal to understanding the current opt-out landscape in the UK. Firstly, GDPR came into force in May 2018 and was fully adopted in the UK, as The Data Protection Act of 2018 (updated to UK GDPR in 2021), despite the UK leaving the European Union. Unlike the earlier UK Data Protection Act of 1988, GDPR explicitly moves towards a legal framework that defaults to opt-out rather than opt-in. The GDPR's overall aim is to increase people's control over their own personal data and 'to protect all EU citizens from privacy and data breaches in an increasingly data-driven world' (EUGDPR 2018). For companies and organisations this means obtaining consent for using and retaining customers' personal data, while granting more rights to the 'data subject' to be informed and control how their personal data is used, as well as to opt out of its use. Secondly, and relatedly, in May 2018 NHS Digital launched its data opt-out programme in line with GDPR guidelines, which aimed to provide 'a facility for individuals to opt out from the use of their data for research or planning purposes' (NHS Digital 2018).

In spring-summer 2018, NHS Digital gradually moved towards full GDPR compliance, updating information, editing website pages, or creating new ones, and operating some of them in 'Beta' mode. Among the latter was the 'NHS Apps Library'. Originally launched in April 2017 (pre-GDPR), aiming to offer '*trusted* digital tools for patients and the public to manage and improve their health' (NHS Apps n.d.: emphasis added), it moved to a 'Beta' version in 2018. Situated within the online NHS environment, the Library (which was still online in 2021, at the time of finishing this book, although in an updated and constantly changing format) was a place where one could assume that the relatively wide range of health apps offered under its umbrella were, as assured, trustworthy and, at the very least, NHS approved. In reality, the NHS Apps Library was a conjunction of competing interests, including commercial ones – the latter including both small businesses and companies developing apps, and the large platform corporations. Beyond the discursive production of trust, at the time of our research in 2018, the App Library existed as a micro-structure, weaving its own independent web of rules that were neither clear, nor necessarily always GDPR or NHS compliant. Furthermore, the notion of 'trust' only partially included the safety of data. For example, the Apps Library offered an 'NHS Badge': a tick that appeared next to a given app as a sign that it had successfully undergone the process of 'Vetting Apps', which resulted in apps being either 'NHS Approved' or 'Being Tested in the NHS'. The text next to 'Being Tested' stated: 'These digital tools meet NHS quality standards for safety, usability and accessibility and are being tested now with NHS patients to see if there is sufficient evidence to provide them an NHS stamp of approval'. The text next to 'NHS Approved' stated: 'This digital tool is NHS Approved. It meets NHS quality standards for clinical effectiveness, safety, usability and accessibility and has a supportive evidence base' (NHS Apps Beta n.d.).

App assessment ensured that the app met 'NHS quality standards for clinical effectiveness, safety, usability and accessibility, and has evidence to support its use'. The NHS assessed an app's 'safety' according to 'both clinical safety and information safety (Information Governance, Privacy and Security)' (Health Developer Network 2018). 'Safety', here, consisted of conjoining and conflating the idea of health risk and data risk. But while the discourse of 'approval'/'vetting' institutionalises user trust via safety scaffolding, supposedly built into the process of verification, the idea of data safety and what it might mean when biodata is aggregated and mined by apps and platforms remained obscure.

The disparity between the Beta version of the online NHS narrative of health app 'safety' and the reality of data safety became apparent when undertaking an examination of the health apps offered by the Library. When reviewed in summer 2018, 43 health apps were offered by the Library but only a few apps had the full NHS Badge. This meant that some apps may have been clinically 'safe' but were subject to information safety breaches, while others may have met information safety standards but not clinical ones. Most of the apps in the library had no badge at all; nor was it clear whether the apps were expected to be GDPR compliant. Most worryingly, despite the narrative of trustworthiness, implicit in the notion of NHS 'vetting', being included in the Library only required a simple five-step online application process. This process only involved answering Digital Assessment Questions and was available to any and all app developers. Upon completion of the application process, apps were added to the Library, regardless of the answers provided (Health Developer Network 2018). In other words, the App Library, which at first glance appeared as *the* database of 'safe' apps for the user/patient to consult, in fact presented a broad spectrum of reliability and safety that obfuscated information about degrees of approval, making it difficult to assess which apps could indeed be fully 'trusted'. To complicate matters, the main audience of the Library was not potential app users but app developers: while the page contained a section called 'Information for Developers', there was no such equivalent for users, who were left to assume responsibility for finding information by themselves.

The Library also did not contain any information about the possibilities of opting out of 'unsafe' – or even 'safe' – apps, after they were installed and activated. The NHS Digital Opt-Out Programme (NHS Digital 2018) was the sole place where opt-out was mentioned. However, its focus was narrow and very particular, relating mostly to the use of data in health care and medical research (NHS Digital 2018). Launched in May 2018 and described as the 'new service that allows people to opt out of their confidential patient information being used for research and planning', the Opt-Out Programme replaced the previous 'type 2 opt-out' which required NHS Digital to refrain from sharing a patients' confidential information for purposes beyond their direct care.[1]

Indexed under 'Systems and Services' and placed in the very long list of other – medical and administrative – services, which can be browsed alphabetically but which are not arranged under any other classification, information on 'opting out' was difficult to find, unless one knew exactly what to look for. The page itself was a mixture of clarity and confusion. On the one hand, information about patient data (purposes and benefits of its collection for health care and medical research; types of anonymised and non-anonymised data; and bodies that would have access to it, such as universities and pharmaceutical companies) and the patient's right to opt out was communicated very clearly. On the other hand, the opt-out itself was cumbersome to execute: users were required to overcome several hurdles, such as clicking through multiple pages, downloading and emailing forms or searching for alternative ways of executing their preferences. Such processes would require not only digital access and literacy, but also time, patience and perseverance – in a striking contrast to how opting in is usually communicated in today's digital environments, where 'download', 'subscribe' and 'follow' buttons are large, immediate and consistently visible.

[1] Type 1 opt-out referred to requests for not sharing one's information beyond direct care, placed directly with the GP and one's local surgery.

Most crucially with regards to this chapter, despite the seemingly clear focus of the Opt-Out Programme, it was not apparent from the Library what exactly the boundaries of patients' rights to opt out were, and whether they encompassed the rapidly growing field of health apps. What were patients opting out *from*? What comprises 'research and planning' mentioned in the NHS data opt-out scheme (NHS Digital 2018)? Research into what? For whose benefit? And how was one's health information being used for this ambiguous purpose? For example, did it apply solely to information collected by on-site GP surgeries and hospitals, or extend to apps providing GP services? Did apps which were 'vetted' by the NHS comply with the NHS Digital Opt-Out Programme? What about apps that were recommended by the NHS but privately owned and run? And what about third parties with which the apps shared their users' data?

Between the Local and the Global, the Legal and the Technical

Moving on from the question of where health apps fit within the broader NHS Opt-Out system, we turn to another conundrum: the relations between national and international legal frameworks, and between legal, corporate and technical regulation. It is crucial to note here that while opt-out is at the heart of GDPR framing of data rights, health apps used in the UK are also part of the global capitalist data economy where such rights are diminishing. How, then, can we understand a European data protection law and (the limits of) its power in the context of global digital platforms and app companies, and their equally global data aggregation? Similarly, what are the impacts and the limits of NHS policies regarding opt-out when they actively collaborate with private, commercial, third-party app providers who may abide by different rules?

One of the ways to consider the conundrum of these geopolitical and socio-legal contradictions was to look at the apps themselves, simultaneously on the level of rhetoric and formal politics *and* on the level of data-related behaviours. In 2018–19, together with a digital health analyst and data visualisation specialist Dr Sam Martin, we studied a selected number of health apps, which seemed NHS-recommended, by either appearing in the NHS Apps Library, or by carrying an 'NHS-endorsed' sign within Apple and Google App stores (Kuntsman et al. 2019). In our analysis, we evaluated, separately and in relation to each other, the following elements: apps' Terms and Conditions and privacy policies as presented on their platforms/websites and within the apps; apps 'permissions' that access other data via one's phone and the tracking of data beyond the app itself; and the way an app handles an opt-out, *after* installation and use.

What we found was telling, not just for research into the UK's health services, but also for any inquiry considering health appisation from the perspective of opting out. We discovered that the information provided about how data was collected, stored and shared, and whether users could request to see their data, varied across the different apps' Terms and Conditions, but was generally limited. Some apps only stated that such information would be confidential, while others provided some partial details of how and with whom the data was shared. Offering an option of opting out of sharing one's information with various affiliates and partners was rare. The apps also differed substantially when it came to their privacy policies, and it was often noted that the information would be shared with third parties. The latter had their own privacy policies, for which the apps in question would not hold any responsibility. Privacy policies, thus, placed the onus on users who were advised to read third party documentation, even though this was often hard to find or navigate.

Even more interesting was the information – or the lack thereof – on the possibility of taking one's data 'out' of the apps after it had been obtained. Could the user request access to information on which data was being collected and held by the app while they were using the app? Could they opt out of sharing some of their data? And finally, could they withdraw their data after deactivation and termination? The apps' legal documents, once again, differed in how broad (or narrow) their opt-out options were. Some allowed only a limited opt-out – for example, from marketing communications. Others offered the opportunity to review, request or delete data, and charged a fee for such services. Opting out of data aggregation, mining and analytics turned out to be complex and confusing. We noted that the continuum of opt-out stretched across different temporalities, as well as across the networked field of data capitalism, often holding user data in opaque traps. For example, some apps allowed users to stop data collection if they wished to discontinue and opt out of the app's services; however, data already collected could not be withdrawn retroactively. Similarly, in some cases, if an app had a 'cooling off' period of thirty days when the decision to discontinue could be reversed, data collection and analytics would continue in the meantime. Furthermore, if data was shared with third parties, an app's policy would not guarantee it would not remain in the hands of those third parties, even if it contained sensitive personal information. All of these scenarios could potentially create 'data ghosts' that continue to feed the mining and analytics profit machine, even after users have withdrawn from the service.

If the legal documentation we analysed was complex, unclear or downright confusing – despite GDPR guidelines dictating that 'data subjects' must be clearly informed before agreeing to give their data – the apps' actual operation made the process of opting out much harder, if not impossible. Firstly, while some apps offered a clear option to leave and discontinue the service from within their interface, others deployed a range of stalling techniques or generally obscured the steps required for disconnection. The process of deactivating the account and deleting all associated data was made cumbersome-by-design, whether on the level of the interface and/or in terms of legal specificities. The labour burden of finding a way out was placed on the user who needed to navigate multiple screens, search for information on deleting a subscription, or go through a multi-step process of completing forms or emailing customer service.

Secondly, as demonstrated by Martin's detailed technical tracing and visualisation of app 'permissions' and data trackers (Martin 2018), when an app was installed on a phone and embedded in the smartphone ecology of other apps, with the ability to share data across the apps and externally, its intrusive analytics were both extensive and not clearly communicated to users. For example, many permissions requested by the app upon installation (such as access to its camera, geolocation, phone calling features or text and phone records) drew excessive additional information, beyond the actual purpose of the app. In addition to being potentially malicious and open to cyber-attacks, these permissions allowed apps to access and share personal data in unclear and obscured ways. To make matters worse, apps also contained a substantial number of trackers, mining data on the way users utilised them, and sharing data with third party analytics. Passing app data to third parties, cross-referencing data with information from other apps on the phone and combining it with behaviour mining via major platforms such as Facebook or Google analytics, had extensive potential for indirect, yet substantial, intrusion into users' privacy and confidentiality.

Finally, and crucially, this complex web of analytics and data sharing required a high degree of legal and technical knowledge, and IT literacy, to understand, modify or opt out of, which most app users do not possess. Opting out, while being a legally defined option, turned out to be a far more complicated process, creating traps that are not only hard to escape, but often difficult to even recognise. And simply leaving or disconnecting was not necessarily an option. Disconnection would be based on a simplistic dichotomy of either accepting the app's rules of the game in their entirety, or deleting the app, and losing the benefits it might offer. However, due to the complexity of data sharing and ownership beyond each individual app, while a 'delete your account' button within an app may have *promised* an easy fix and a full and *finite* opt-out, the reality of opting out of data traps, once a person had started using the app, was complicated and uncertain. This complexity was and is both individual and geopolitical. Whilst apps' data draws on locality and individuality at a level of an individual patient/user (for example, collecting data on specific personal health conditions, geolocation or local social and health networks), they also operated within global data flows that are governed by international platforms, often headquartered in the US. These platforms' data governance extends beyond the socio-legal jurisdictions of a given locality and country of practice. For example, at no point was it clear to the user whether and how GDPR might come into play when one's data is housed in the US or passed to multiple third parties around the globe. We argue that the architecture of technical obfuscation – such as the one involved in the process of individual opting out – is intertwined with multiple socio-legal grey areas and loopholes that disperse personal data into a collective Big Data pool. Together, they operate as what Pasquale (2016) described as a 'black box society', where techno-social processes that are central to our everyday life operate beyond any individual user's comprehension or power to control it.

Contact Tracing Apps and Performative Data Consciousness

Two years after GDPR was introduced, the question of opting out of digital health faced a new, unprecedented challenge. In light of the Covid-19 pandemic, concerns about privacy, data profiling and the monetisation of personal data were both heightened *and* expected to take a back seat, as government after government across the globe introduced 'contact tracing' apps to map, record, analyse and control the spread of coronavirus infections. The apps, developed in the early months of the pandemic, were introduced in many countries throughout 2020. While some countries or contexts made the use of the apps compulsory for all citizens, or for those travelling through its borders (AccessNow 2020; Schmid 2020), in other countries the use of contact tracing apps was optional but highly encouraged.

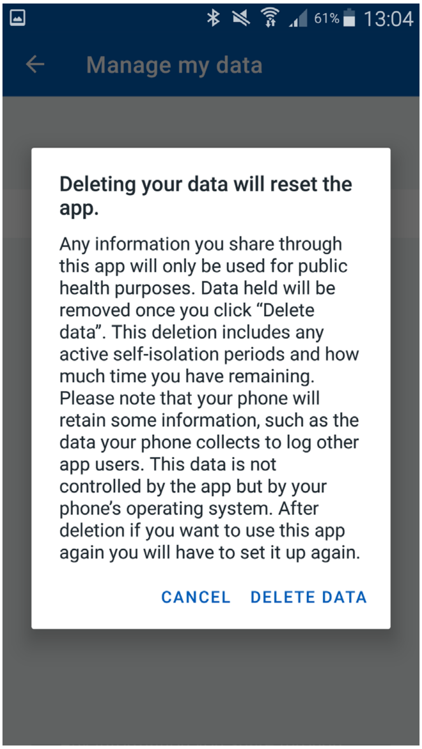
From the moment of their inception, the apps attracted concerns from journalists, human rights activists and academics for their potential to result in expanded state surveillance and corporate control (Das 2020; Everts 2020; French and Monahan 2020; Kitchin 2020; Kouřil and Ferenčuhová 2020; O'Neill et al. 2020; van Kolfschooten and de Ruijter 2020; Yu 2020); together with proactive suggestions of how to navigate what Kitchin called the tension between civil liberties and public health (2020). In May 2020, the MIT Technology Review created a 'Covid Tracing Tracker' – a database on contact tracing apps, including details about how they work and which policies are in place to govern them (O'Neill et al. 2020). Several scholars published rapid response papers, analysing contact tracing apps from the perspective of their efficiency (or lack thereof), geographic distribution, biopolitics of control and the need to make the apps' operation more transparent especially in relation to personal details aggregated in state-controlled databases (Das 2020; Everts 2020; French and Monahan 2020).

The UK was among the late adopters of a contact tracing app. After lengthy deliberations and months of operating a chaotic and often dysfunctional non-app contact tracing system, in September 2020 the 'NHS COVID-19' contact tracing app was finally launched in England and Wales, with separate apps operating in Scotland ('Protect Scotland') and Northern Ireland ('StopCovidNI'). Contrary to fears about increased surveillance, which dominated media coverage in spring 2020, most reports about NHS COVID-19, in both mainstream and social media, were about the app *not* working properly – not installable on older models of Android and iPhones (Hern 2020a); not working in some languages (Hern 2020b); incorrectly reporting the risk levels (Hern 2020c; PapacassKitchen 2020); or sending erroneous exposure alerts to people who barely left their homes (Payne 2020).

When we carried a 'walk through' (Light, Burgess and Duguay 2018) analysis of the NHS COVID-19 app, which included app installation and use, we noted that the interface appeared simple and straightforward. The information on privacy, confidentiality and the rationale for data collection was presented very clearly, for example, explaining why postcode data was required upon registration; why geolocation or Bluetooth needed to be switched on for the app to operate – and that these could always be temporarily switched off at the user's discretion; or how long one's data was kept. Information on withdrawing one's data was also clearly presented and relatively easy to find and execute – in a striking contrast to other health apps we had researched previously.

All the above suggests that the app's interface was continuously performing what may seem like high-level privacy awareness, perhaps in an attempt to alleviate public concerns in light of multiple media reports of heightened surveillance through contact tracing in other countries. The user was repeatedly assured that their privacy was protected and information on their infections or exposures was confidential and anonymised, and was not retained after an opt-out. These assurances, however, were limited to the app alone – as the 'deleting your data' screenshot shows (Figure 1.1), for example, the data was not controlled by the app but by the phone – and here the app's responsibility ended. Beyond this statement, little explanation was given as to what 'data control by the phone' actually meant or how user data was mined by bodies other than the app itself, for instance via in-phone interactions as detailed earlier in this chapter.

In fact, the app's interface provided an *illusion* of control, by allowing the user to temporarily opt out of being traced, by switching the contact tracing function on and off as desired – which might make the user feel as if they could temporarily make themselves invisible. This is in striking contrast to fears regarding the dangers of contact tracing technology – that it could lead to stalking or cybercrime, or would intensify state surveillance of citizens by tracking every move at every given moment – as indeed is the case with contact tracing apps in some countries. However, what remained unacknowledged was the ways in which the app's opt-out options facilitated other forms of data mining, which were not related to coronavirus tracking, nor to the app itself, while ostensibly providing an opt-out optionality. For example, when switching the contact tracing function (back) on, geolocation and Bluetooth were turned on by the app. Yet, when contact tracing was switched off from *within the app*, both geolocation and Bluetooth remained active on the phone, and needed to be switched off manually. Without knowing or remembering to do so, the phone and its data were made more visible and more minable, trapping more data than the user may have ever agreed to; all the while the user may have felt 'invisible' and empowered. Once again, the opt-out of the smartphone *ecology* of data mining was far less straightforward than clicking the 'off' button, making the performance of data consciousness an empty gesture.



Deleting your data will reset the app.

Any information you share through this app will only be used for public health purposes. Data held will be removed once you click "Delete data". This deletion includes any active self-isolation periods and how much time you have remaining. Please note that your phone will retain some information, such as the data your phone collects to log other app users. This data is not controlled by the app but by your phone's operating system. After deletion if you want to use this app again you will have to set it up again.

Figure 1.1: Deleting your data. Phone screenshot. Collected 16.10.20 (Source: Adi Kuntsman).

Individual and Collective Opt-Outs

Since the introduction of GDPR, it could be argued that the move to become 'GDPR-compliant' is a step forward towards increased transparency and an improvement in the digital rights of health apps' users, where opting out is becoming institutionalised. As we can see in the case of the NHS contact tracing app, it can even be clearly embedded into the app's interface. Yet a closer look at how such compliancy is implemented – not just through everyday practices, but also at a more granular and algorithmic level of health apps and smartphone ecologies – reveals a fluid and complex web of networked 'data traps' for which no single app could be held responsible. In that respect, GDPR as the legal framework, *and* some apps being seemingly data conscious (such as NHS COVID-19) is both empowering *and* confusing due to the illusion of protection they offer to individual users. Practices and technologies of opting out struggle to find a place within a context that is simultaneously part of the global capitalist data and platform economy, where opt-out rights are diminishing and personal data is shared easily and excessively, *and* is subject to a new regional and national data protection regulation which places opt-out rights at its centre.

However, a further conundrum is in place: one between individual and collective opt-outs. The process of appisation, which is based on having an *individual* gadget and an *individual* account to support one's health, signals the increasing individualisation and self-responsibilisation of health: self-care, self-management, self-tracking and self-monitoring (Ajana 2017; Kristensen and Ruckenstein 2018; Lupton 2014; Lupton 2016; Neff and Nafus 2016; Sharon and Zandbergen 2017). The process is true for both those contexts where health care is private, and where it is nationalised and free, albeit crumbling – as in the UK.[2] Digital health, then, seems to be about empowering the individual, where responsibility and accountability of one's own health now includes responsibility for one's own personal data: the onus of safeguarding, accepting, refusing and determining ways out always falls to the individual user. And here, the management of one's data is often presented with an *illusion of choice*. This is particularly apparent in how the App Library interpolates the 'you' and the 'self' (Althusser 1971/2001), and in practices such as accepting Terms and Conditions, or in granting app permissions, not to mention the very decision to choose and install an app – an epitome of agentic 'consumer choice' (Bauman 2001; Bol et al. 2018; Borgerson 2005; Schwarzkopf 2018). Even during the Covid-19 pandemic, when concerns about individual freedoms were deemed secondary to the collective cause of fighting coronavirus globally, the app focuses on the individual who seemingly has a choice at every step. At the same time, health apps bring a radically new level of data powerlessness. When health information is shared, and jointly mined, with a search/advertising engine (such as Google) or a social media site (such as Facebook), 'doctor patient confidentiality' becomes all but a symbolic gesture from bygone days. Health appisation gives rise to algorithmic 'care', one based on analytics that might be more efficient, speedy and precise, yet is also relentlessly intrusive and non-private, where no medical information is left untouched, unseen or undisclosed.

[2] Although of course, the relations between healthcare affordability and the use of health apps is an important topic to explore. For example, we would expect there to be a difference between a free app (or an app with very affordable subscription costs), which is used by those unable to afford regular healthcare, and an app that is used to complement a free national health care system. One might speculate whether surrendering one's data in return for what seems to be a free medical service would be seen as more acceptable and even welcome by some. Similarly, we can investigate the profit from app subscription charges versus those from data monetisation; how the two types of profit are made clear or invisibilised, and whether/how both forms of app capitalism are understood and legitimated. These are questions that require further research, which is beyond the scope of our book.

More crucially, the broad and extensive sharing of personal (bio)data for analytics and profit means that opting out of, or the use of, health apps is first and foremost about large-scale *collective* datafication and the economy of surveillance capitalism (Zuboff 2019). The latter is still not fully understood by the public, especially when juxtaposed with political/state surveillance. The debates that preceded the launch of the UK's NHS COVID-19 app are a telling example. Before the introduction of the app in September 2020, extensive deliberations took place regarding its design and data management. Initially, the NHSX app was to be adapted to contact tracing, using centralised technology where the data would be hosted centrally on NHS computer servers (Downey 2020). However, the adaptation was delayed, largely due to concerns about privacy and data safety. Eventually, Apple and Google 'decentralised' technology was adopted instead in the development of what became the NHS COVID-19 app, because their contact tracking technology was deemed to be less intrusive (Kelion 2020). Such a dichotomy gestures to a severely limited understanding of data power and surveillance capitalism, where surveillance by the state or national health services is deemed intrusive, whereas dispersed but extensive data mining by major platforms appears 'safer' – even though opt-out of the latter, as we have shown, is all but impossible.

The focus on individual privacy and individual data safety – in the context of contact tracing and more broadly – brings our attention to the conundrum of (seeming) individual data empowerment versus collective data powerlessness that is at the heart of health appisation. While data and privacy management practices are individual, and targeted advertising is also individually tailored, the individual is meaningless in the eyes of algorithmic determinism and prediction. A single user's data has no representative value: monetary and statistic capital lies with aggregated *Big* Data. The digitisation of health exists in the tension between the neoliberal model of the individual whose health and data concerns are personalised into the 'Self', and the digital capitalist model (Fuchs 2010; Fuchs 2014; Fuchs 2015; Schiller 2000), which generates value in the collective (and thus, representationally and statistically 'valid') data of the masses. It is here that we witness what Ajana coined the shift 'from individual data to communal data, from the Quantified Self to the 'Quantified Us', from the 'biopolitics of the self' to the biopolitics of the population' (Ajana 2017).

Within such a context, 'opting out' is subject to oppositional forces: it is a matter of individual rights (and responsibilities) while also, paradoxically, situated within a system that supports, and capitalises on, *mass* value and *mass* data. Legal changes, such as GDPR, are undoubtedly a welcome and much-needed attempt to protect individual rights in the world of large-scale data sharing, mining and profiling. Yet, in addition to exploitable loopholes within supposedly GDPR-compliant apps, which might endanger the individual or even entire national or regional legal frameworks – loopholes that need to be exposed and mended – a more substantial issue is at stake regarding the effectiveness of legal frameworks such as GDPR. When the digital data economy traffics in Big Data, and when, concurrently, individual data ownership erodes in favour of 'data philanthropy'– a growing shift towards 'surrendering' one's data for the 'public good', where unwillingness to share and concerns for privacy are seen as 'selfish and anti-solidaristic' (Ajana 2017) – legally addressing *individual* responsibility and *individual* protection is not enough and will never be fully sufficient.

Conclusion: From Data Rights to Data Justice

How, then, can we approach, analyse and change the current landscape of the 'socio-cultural data traps' of health apps, and the shrinking space of data opt-out? As a first step, we argue, individual app users and medical and health care providers involved in the digitisation of health need to equip themselves with socio-political *and* technical tools for understanding, mapping and monitoring the datafied operation of health apps. Secondly, and crucially, we must also reframe opting out itself as a matter of 'data justice', and not just a data 'right', one that is placed at the centre of considering the entire data *ecology* and data *economy*, rather than merely addressing individual practices of one user in relation to one app. Here, we align our conceptualisation of digital disengagement with the emerging body of scholarship on 'data justice' (Dencik et al. 2016; Johnson 2014; Iliadis 2018; Taylor 2017) which, as Taylor formulates, should include 'the freedom not to use particular technologies, and in particular not to become part of commercial databases as a by-product of development interventions' (Taylor 2017, 9). Taylor's call is particularly relevant today, where the large-scale, rapid initiatives of digital contact tracing create a substantial commercial gain for both the firms involved in developing the apps, and the large platforms whose decentralised technology is being used.

In order to create a space for both individual rights to refuse to be part of a database (Taylor 2017) and a more systemic, collective refusal of 'biopolitical categorisations that are enabled through Big Data practices' (Ajana 2017, 13), we need to acknowledge that focusing on individual data rights – including the right to opt out – is not and will not be enough. To challenge the structural nature of health apps' data traps, we need to move away from the biopolitics of health commodification more broadly. This does not mean refusing the use of digital technologies in public or community health services. Rather, this is about moving to decoupling equal and just health provision from a compulsory dependency on non-medical digital communication. And when digital tools are truly and urgently needed (and might outweigh individual concerns about privacy, such as in the case of an epidemic), they must be adopted in a thoughtful and transparent way, instead of merely assuming they will work, or are indeed the best solution. Digitisation that is attentive not only to individual rights but to collective data justice must purposefully strive to avoid exclusionary and discriminatory data harms, on the one hand, and profit-driven data grabs, on the other. In the next chapter, we explore the rift between individual digital rights and collective digital justice further, by looking at digitisation, social mediatisation and algorithmic automation of decision-making in public services, policing and border control.

Bibliography

AccessNow. 2020. 'UNGA 75 Side Event: COVID-19, Surveillance, and the Right to Privacy'. AccessNow. 2 October. https://www.accessnow.org/unga-75-side-event-covid-19-surveillance-and-the-right-to-privacy/

Ajana, Btihaj. 2017. 'Digital Health and the Biopolitics of the Quantified Self'. *Digital Health*, 3. https://doi.org/10.1177/2055207616689509

Althusser, Louis. 2001. *Lenin and Philosophy, and Other Essays*. New York: Monthly Review Press. (Original work published 1971).

Babylon. 2016. *Babylon Health*. https://www.babylonhealth.com/

Bauman, Zygmunt. 2001. 'Consuming Life'. *Journal of Consumer Culture*, 1 (1): 9–29. https://doi.org/10.1177/146954050100100102

Bol, Nadine, Natali Helberger, and Julia C. M. Weert. 2018. 'Differences in Mobile Health App Use: A Source of New Digital Inequalities?' *The Information Society*, 34 (3): 183–93. https://doi.org/10.1080/01972243.2018.1438550

Borgerson, Janet L. 2005. 'Materiality, Agency, and the Constitution of Consuming Subjects: Insights for Consumer Research'. *Advances in Consumer Research*, 31: 439–43.

Cinnamon, Jonathan. 2017. 'Social Injustice in Surveillance Capitalism'. *Surveillance & Society*, 15 (5): 609–25. https://doi.org/10.24908/ss.v15i5.6433

Culture Health and Wellbeing Alliance. n.d. 'Social Prescribing. Culture Health and Wellbeing'. https://www.culturehealthandwellbeing.org.uk/resources/social-prescribing

Das, Soumyo. 2020. 'Surveillance in the Time of Coronavirus: The Case of the Indian Contact Tracing App Aarogya Setu'. *Datactive*. 30 April. https://data-activism.net/2020/04/bigdatasur-covid-surveillance-in-the-time-of-coronavirus-the-case-of-the-indian-contact-tracing-app-aarogya-setu/

Dencik, Lina, Arne Hintz, and Jonathan Cable. 2016. 'Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism'. *Big Data & Society*, 3 (2). https://doi.org/10.1177/2053951716679678

Downey, Andrea. 2020. 'NHS Differs with Apple and Google over Contact-Tracing App'. *Digital Health*. 30 April. https://www.digitalhealth.net/2020/04/nhsx-differs-with-apple-and-google-over-contact-tracing-app/

EUGDPR. GDPR Key Changes. 2018. Last accessed 1 June 2018, https://www.eugdpr.org/key-changes.html. Internet Archive. https://web.archive.org/web/20180608003143/https://www.eugdpr.org/key-changes.html

Everts, Jonathan. 2020. 'The Dashboard Pandemic'. *Dialogues in Human Geography*, 10 (2): 260–64. https://doi.org/10.1177/2043820620935355

French, Martin, and Torin Monahan. 2020. 'Dis-Ease Surveillance: How Might Surveillance Studies Address COVID-19?' *Surveillance & Society*, 18 (1): 1–11. https://doi.org/10.24908/ss.v18i1.13985

Fuchs, Christian. 2010. 'Labor in Informational Capitalism and on the Internet'. *The Information Society*, 26 (3): 179–96. https://doi.org/10.1080/01972241003712215

Fuchs, Christian. 2014. *Digital Labour and Karl Marx*. New York: Routledge.

Fuchs, Christian. 2015. *Culture and Economy in the Age of Social Media*. New York: Routledge.

Gardner, Howard, and Katie Davis. 2013. *The App Generation: How Today's Youth Navigate Identity, Intimacy, and Imagination in a Digital World*. New Haven: Yale University Press.

Health Developer Network. 2018. Digital Assessment Questions – Beta. Developer NHS. https://developer.nhs.uk/digital-tools/daq/. Internet Archive. https://web.archive.org/web/20180307091740/https://developer.nhs.uk/digital-tools/daq/

Hern, Alex. 2020a. 'Users Report Issues as Covid-19 App Launches in England and Wales'. *The Guardian*, 24 September. https://www.theguardian.com/world/2020/sep/24/users-report-issues-as-covid-19-app-launches-in-england-and-wales

Hern, Alex. 2020b. 'NHS Covid App Does Not Work for Phones Set to French and Spanish'. *The Guardian*, 28 October. https://www.theguardian.com/world/2020/oct/28/nhs-covid-app-does-not-work-for-phones-set-to-french-and-spanish

Hern, Alex. 2020c. 'Fault in NHS Covid App Meant Thousands at Risk Did Not Quarantine'. *The Guardian*, 2 November. https://www.theguardian.com/world/2020/nov/02/fault-in-nhs-covid-app-meant-thousands-at-risk-did-not-quarantine

Iliadis, Andrew. 2018. 'Algorithms, Ontology, and Social Progress'. *Global Media and Communication*, 14 (2): 219–30. https://doi.org/10.1177/1742766518776688

Johnson, Jeffrey Alan. 2014. 'From Open Data to Information Justice'. *Ethics and Information Technology*, 16 (4): 263–74. https://doi.org/10.1007/s10676-014-9351-8

Juhila, Kirsi, Suvi Raitakari, and Christopher Hall. 2017. *Responsibilisation at the Margins of Welfare Services*. Abingdon: Routledge.

Kelion, Leo. 2020. 'UK Virus-Tracing App Switches to Apple-Google Model'. *BBC News*, 18 June. https://www.bbc.co.uk/news/technology-53095336

Kitchin, Rob. 2020. 'Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19'. *Space and Polity*, 24 (3): 362–81. https://doi.org/10.1080/13562576.2020.1770587

Kouřil, Petr, and Slavomíra Ferenčuhová. 2020. '"Smart" Quarantine and "Blanket" Quarantine: The Czech Response to the COVID-19 Pandemic'. *Eurasian Geography and Economics*, 61 (4–5): 587–97. https://doi.org/10.1080/15387216.2020.1783338

Kristensen, Dorthe Brogård, and Minna Ruckenstein. 2018. 'Co-Evolving with Self-Tracking Technologies'. *New Media & Society*, 20 (10): 3624–40. https://doi.org/10.1177/1461444818755650

Kuntsman, Adi, Esperanza Miyake, and Sam Martin. 2019. 'Re-thinking Digital Health: Data, Appisation and the (Im)Possibility of "Opting Out"'. *Digital Health*, 5. https://doi.org/10.1177/2055207619880671

Lehtiniemi, Tuukka. 2017. 'Personal Data Spaces: An Intervention in Surveillance Capitalism?' *Surveillance & Society*, 15 (5): 626–39. https://doi.org/10.24908/ss.v15i5.6424

Light, Ben, Jean Burgess, and Stefanie Duguay. 2018. 'The Walkthrough Method: An Approach to the Study of Apps'. *New Media & Society*, 20 (3): 881–900. https://doi.org/10.1177/1461444816675438

Lucas, Henry. 2015. 'New Technology and Illness Self-Management: Potential Relevance for Resource-Poor Populations in Asia'. *Social Science & Medicine*, 145: 145–53. https://doi.org/10.1016/j.socscimed.2014.11.008

Lupton, Deborah. 2014. 'Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps'. *Societies*, 4 (4): 606–22. https://doi.org/10.3390/soc4040606

Lupton, Deborah. 2016. 'Digitized Health Promotion: Personal Responsibility for Health in the Web 2.0 Era'. In Joseph E. Davis and Ana Marta González (Eds.). *To Fix or to Heal: Patient Care, Public Health, and the Limits of Biomedicine* (pp. 152–76). New York: New York University Press.

Martin, Sam. 2018. 'Rethinking Digital Health Opt-Out: Smartphone Trackers'. https://digitalcoeliac.com/rethink-dh2018/

Miller, Paul D., and Svitlana Matviyenko. (Eds.). 2014. *The Imaginary App*. Cambridge: MIT Press.

Morris, Jeremy Wade, and Sarah Murray. (Eds.). 2018. *Appified: Culture in the Age of Apps*. Ann Arbor: University of Michigan Press.

Morton, Katherine, Laura Dennison, Carl May, Elizabeth Murray, Paul Little, Richard J. McManus, and Lucy Yardley. 2017. 'Using Digital Interventions for Self-Management of Chronic Physical Health Conditions: A Meta-Ethnography Review of Published Studies'. *Patient Education and Counseling*, 100 (4): 616–35. https://doi.org/10.1016/j.pec.2016.10.019

Neff, Gina, and Dawn Nafus. 2016. *Self-Tracking*. Cambridge: MIT Press.

NHS Apps. n.d. NHS Apps Library. NHS Apps Library. Last Accessed 5 June 2018, https://digital.nhs.uk/services/nhs-apps-library

NHS Apps Beta. n.d. NHS Apps Library: About Us. Apps Beta NHS. https://apps.beta.nhs.uk/about-us/. Internet Archive. https://web.archive.org/web/20180921025110/https://apps.beta.nhs.uk/about-us/

NHS Digital. 2018. National Data Opt-Out Programme. https://digital.nhs.uk/services/national-data-opt-out-programme

NHS Digital. n.d. NHS Digital. Digital NHS. Last accessed 1 June 2018, https://digital.nhs.uk/

NHS Digital. n.d. Systems and Services. https://digital.nhs.uk/services/a-to-z

O'Neill, Patrick Howell, Tate Ryan-Mosley, and Bobbie Johnson. 2020. 'A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them'. *MIT Technology Review*, 7 May. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Øvretveit, John. 2015. 'Improving Quality with Digital Health Technology Supporting Coordination and Self-Care: Findings from 4 EU Countries in the EU Integrate Project'. *International Journal of Integrated Care*, 15 (5). https://doi.org/10.5334/ijic.2134

PapacassKitchen. 2020. Twitter Post, 16 October. https://twitter.com/PapacassKitchen/status/1317198847316234241?s=20

Pasquale, Frank. 2016. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Payne, Will. 2020. 'NHS Test and Trace Tell Strood Family to Self-Isolate Even Though They Haven't Left Home for Weeks'. *Kent Online*, 3 December. https://www.kentonline.co.uk/medway/news/family-told-to-isolate-despite-not-leaving-home-for-three-weeks-238491/

Schiller, Dan. 2000. *Digital Capitalism: Networking the Global Market System*. Cambridge: MIT Press.

Schmid, Joseph. 2020. 'Virus Tracing Apps: Which Countries Are Doing What'. *Medical Xpress*, 29 May. https://medicalxpress.com/news/2020-05-virus-apps-countries.html

Schwarzkopf, Stefan. 2018. 'Consumer-Citizens: Markets, Marketing and the Making of "Choice"'. In Olga Kravets, Pauline Maclaran, Steven Miles, and Alladi Venkatesh (Eds.). *The Sage Handbook of Consumer Culture*. Thousand Oaks: SAGE Publications.

Sharon, Tamar, and Dorien Zandbergen. 2017. 'From Data Fetishism to Quantifying Selves: Self-Tracking Practices and the Other Values of Data'. *New Media & Society*, 19 (11): 1695–1709. https://doi.org/10.1177/1461444816636090

Silverman, Jacob. 2017. 'Privacy under Surveillance Capitalism'. *Social Research: An International Quarterly*, 84 (1).

Taylor, Linnet. 2017. 'What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally'. *Big Data & Society*, 4 (2): 1–14. https://doi.org/10.1177/2053951717736335

van Dijck, José, and Thomas Poell. 2016. 'Understanding the Promises and Premises of Online Health Platforms'. *Big Data & Society*, 3 (1). https://doi.org/10.1177/2053951716654173

Van Kolfschooten, Hannah, and Anniek de Ruijter. 2020. 'COVID-19 and Privacy in the European Union: A Legal Perspective on Contact Tracing'.

Contemporary Security Policy, 41 (3): 478–91. https://doi.org/10.1080/13523260.2020.1771509

Yu, Ai. 2020. ‘Digital Surveillance in Post-coronavirus China: A Feminist View on the Price We Pay’. *Gender, Work & Organization*, 27 (5): 774–77. https://doi.org/10.1111/gwao.12471

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. London: Profile Books.