Fit for purpose? The GDPR and the governance of European digital health

Luca Marelli, Elisa Lievevrouw & Ine Van Hoyweghen

Abstract

The introduction of the General Data Protection Regulation (GDPR) in 2018 served as the cornerstone of the new data governance regime of the European Union. Informed by principles and values such as privacy, accountability, transparency, and fairness, the GDPR is premised on the objective to balance the protection of individual privacy and the promotion of a thriving European data economy. Still, shortcomings of this regulatory effort have been noted by recent ethical, socio-political, legal, and policy scholarship. Focusing on the deployment of digital health technologies and big data practices within the European digital health ecosystem, this article draws upon these bodies of literature to chart the main lines of tension emerging between the current GDPR-based data governance regime and the broader societal shifts coming along with the expansion of digital health. Central aspects of the GDPR–i.e. key underlying data protection principles and regulatory categories, the reliance on the "notice- and-consent" model, the (narrow) remit of the Regulation vis-à-vis possible harms and discriminations–are misaligned with the surge in digital health. This throws into doubt whether the Regulation is fully fit for the purpose of governing current developments in this field, while also calling for swift and adequate policy responses.

Introduction

In recent years, digital health (DH) has acquired priority status in the health policy agenda, being widely embraced by tech industry leaders while also gaining ground in national and international innovation policy discourses. Predicated on advances in fields such as "precision" or "personalized" medicine, big data analytics and mobile Health (mHealth), DH has been mobilized as a panacea for healthcare systems worldwide (Lievevrouw and Van Hoyweghen 2019), whose long-run sustainability is considered threatened by rising costs, budgetary constraints, as well as the growing prevalence of chronic diseases and population aging (EC 2018; IMI 2014; WHO 2017, 2019a).

DH innovation strategies have been launched by a variety of governments and supra- national institutions, from Australia (Australian Digital Health Agency 2018) to the European Union (EU) (EC 2018), from Japan (Kumar 2019) to Singapore (Ministry of Health Singapore 2019). In the regulatory domain, the United States' Food and Drug Administration (FDA) was a frontrunner in promoting changes to medical device approval procedures, with the aim of tailoring regulatory standards for safety and efficacy to the specificities of DH (FDA 2013; Gottlieb 2018). Likewise, changes have been made to EU regulations of medical devices (Official Journal of the European Union 2017a) and in vitro diagnostic medical devices (Official Journal of the European Union 2017b), which now also embed "software" into the definition of

"medical device" and thus extend the medical device approval system to digital health technologies (DHTs) (Ordish, Hannah, and Allison 2019).

In the meanwhile, several European states have developed good practices guidelines for developers and evaluators, to ensure the quality and safety of non-medical device DHTs (e.g. France), to clarify the demarcation between DH medical devices and consumer technologies (e.g. UK), and to develop a DH-specific risk-classification system (e.g. Germany) (Haute Autorité de Santé 2016; IGES Institute 2016; Medicines and Healthcare products Regulatory Agency 2014). Moreover, changes to policies geared to enable the reimbursement of DHTs by public healthcare systems have been brought forth by the German parliament (Federal Ministry of Health 2019) and the National Institute for Health and Care Excellence in the UK (NICE 2019).

At the supranational, EU level, following the Green paper on "Mobile Health" (EC 2014b) and a "Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps" (EC 2014a), the European Commission has identified the implementation of DH as a primary policy objective. This has been reflected in various EU-level policy initiatives, including the creation of a European cooperation mechanism for genomic and health data sharing (Saunders et al. 2019), as well as the development of a European electronic health record exchange format (EC 2018). At its core, the development and increased circulation of DHTs is envisaged by the European Commission to strengthen the "resilience and sustainability" of Europe's health and care systems (EC 2018, 4). Moreover, it is meant to "maximize the potential of the digital internal market with a wider deployment of digital pro- ducts and services" (EC 2018, 4), and to contribute to the growth of the European data economy.

In parallel to these developments, in 2016 the European Parliament approved Regulation (EU) 2016/679 on data protection, also known as the General Data Protection Regulation (GDPR) (Official Journal of the European Union 2016). The passing into law of the GDPR came after a contentious approval process shaped by intense lobbying efforts on the part of (mostly US) Big Tech corporations, as well as underlying conflicts among EU member states, diverging in economic interests and cultural perceptions over privacy and data protection (Mager 2017). Replacing the previous, two decades-old data protection directive (Official Journal of the European Communities 1995), the GDPR set out to harmonize data protection legislation in the EU;1 by adopting an "omnibus", rather than sectoral, approach to data protection, the GDPR is also intended to cover a wide scope of processing areas, including DH, while implementing a flexible, context-sensitive and risk-based governance strategy that foregrounds breadth of reach and the accountability of data controllers vis-à-vis granularity and specificity in the (sub-sectoral) application of its provisions (Marelli and Testa 2018).

Enforced since May 2018, this Regulation has come to represent the cornerstone of the new data governance regime of the European Union. As remarked by its rapporteur at the European Parliament, former German MEP Jan Albrecht, the GDPR is premised on the objective to reconcile two competing requirements, that is, to provide

> the right balance between a high level of protection for the fundamental right to data protec- tion as well as strong consumer rights in the digital age, on the one side, and the need to create

> a fair and functioning digital market, with a real chance for growth and innovation, on the other side. (Albrecht 2016a)

In so doing, the GDPR has been put forward as an important lever for advancing "the European way" to digital innovation, tailored to what are framed as distinctive European values and principles such as privacy, accountability, transparency, and fairness.

Recently, a number of expert opinions and socio-political, ethical, legal, and policy studies have started to draw attention to the shortcomings of this Regulation. A number of important concerns pertain to the ability of the GDPR to adequately address the issues raised by the European digital data economy, and to reduce the risks for people and society. At their core, these arguments point to the difficulties of transitioning from a data governance model rooted in a pre-digital world to one tailored to our "post-digital" societies, which are characterized by the ubiquitous diffusion of digital technologies. As Mayer-Schönberger and Padova have argued in this regard, the GDPR represents in fact "a stepping stone, pointing towards the need to evolve data protection beyond the old paradigm, yet not fully committed to doing so" (Mayer-Schönberger and Padova 2016, 332).

In this article, we draw upon this expanding body of literature and focus on arguments that have either been specifically advanced for, or can be also applied to, the field of DH. We do so to chart the main lines of tension emerging between the GDPR-based data governance regime and the broader societal shifts coming along with the proliferation of DHTs and big data practices in the health domain. In what follows, we first outline, and discuss the implications of, these broader societal shifts. Next, we identify four main areas (Table 1) where data protection standards advanced by the GDPR appear misaligned and in tension with current developments in digital health. In turn, by reviewing these tensions, we raise the question of whether the GDPR, in spite of its widely praised approach geared to balance individual protection and economic growth, is in fact fully fit for the purpose of governing the rapid expansion of DH; or whether, on the contrary, its shortcomings could lead to unintended con- sequences, either in terms of depriving European citizens of adequate protection, or potentially curbing the further expansion of the European digital health ecosystem and the societal benefits potentially associated with it.

The societal performativities of DHTs

Policymakers, practitioners and scholars alike typically refer to DH in wide-encompassing terms. The World Health Organization (WHO) understands DH to be "a broad umbrella term encompassing eHealth (which includes mHealth), as well as emerging areas, such as the use of advanced computing sciences in 'big data', genomics and artificial intelligence." (WHO 2017, 1). In a similarly broad fashion, the FDA defines DHTs in relation to

Table 1. Misalignments between digital health practices and the GDPR.

DH practices	GDPR's standards challenged by DH practices
▪ New technological affordances (e.g. machine learning): ⇒ repeated and combinatorial use of data ⇒ impossibility to identify purposes at time of data collection ⇒ opacity of algorithms ▪ New actors, corporate digital platforms: ⇒ re-purposing of datasets and context transgression ⇒ opacity of corporate business models	**Data protection principles:** ▪ "Purpose limitation" ▪ "Data minimization" and "storage limitation" ▪ "Transparency"
▪ "Lifestylization of healthcare" and use of health data outside healthcare institutions: ⇒ "regular" data types convey sensitive information ⇒ context transgression ▪ New technological affordances (e.g. predictive and inferential analytics): ⇒ "regular" data types convey sensitive information ▪ Open access genomic databases ⇒ de-anonymization of datasets	**Key categorial distinctions:** ▪ Sensitive / non-sensitive data ▪ Identifiable / non- identifiable (anonymous) data
▪ Unintelligibility and/or vagueness of privacy notices: ⇒ lack of transparency ⇒ "transparency paradox" ▪ "Opt-in vs. opt-out" choice in DH platforms: ⇒ highly constrained choices, passive acquiescence when consenting ⇒ propensity for easily waiving privacy rights	**Informational self-determination approach:** ▪ Notice-and-consent model
▪ Predictive modelling and risk scores, social sorting: ⇒ Algorithmic discriminations and privacy harms	**(Narrow) scope of the Regulation:** ▪ Focus on the individual data subject ▪ Narrow legal remit

"categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine" (FDA 2019). From the analyst's perspective, Lupton identifies person-centeredness and self-care as defining features of DH (Lupton 2018, 1)2, while other scholars, such as Petersen, foreground the deployment of advanced information technologies in the health domain, defining DH as "a kind of healthcare that is increasingly big data-driven, using artificial intelligence (AI), algorithms and machine learning to undertake healthcare decisions." (Petersen 2019, 2).

In this article, we build on the broad meaning of DH. Following Hoeyer, who identifies "intensified data sourcing" (Hoeyer 2016, 74) as a defining tenet of contemporary practices in DH, we focus on the data processing and datafication side of DHTs. The latter are guided by the aim of continuously "getting more data, of better quality, on more people", while "simultaneously making them available for multiple purposes, including research, governance and economic growth" (ibid.). These features, in turn, trigger

broader societal reconfigurations, which mostly revolve around the emergence of new actors, spaces, and classificatory practices.

First, the rapid expansion of the "digital health ecosystem" (Vayena et al. 2018; WHO 2019b) has been largely driven by the inclusion of new types of actors within traditionally bounded institutional spaces. Following in the footsteps of early initiatives such as Apple's ResearchKit, Samsung's Simband, and Google's Verily and DeepMind, large consumer technology corporations in particular have started making conspicuous inroads into the domain of health research and care. Advancing a vision of disruptive change of established practices and values around health research and delivery (Powles and Hodson 2017; Wingfield, Thomas, and Abelson 2018), these corporations have harnessed their consider- able resources to position themselves as "obligatory passage points" in research networks (Sharon and Lucivero 2019), and have further broadened their scope by delving into the organization and direct provision of healthcare and health insurance (Farr 2018; Wingfield, Thomas, and Abelson 2018). The implications of this "Googlization" of health research and care (Sharon 2016) can be felt at multiple levels. At their core, large-scale, corporate-owned digital platforms have been shown to import into the health domain political-economic dynamics – such as market-dominance, and the creation of divides between the "data haves" and the "data have nots" (see e.g. Andrejevic 2014; Boyd and Crawford 2012; Prainsack 2019; van Dijck, Poell, and de Waal 2018) – which are typical of emerging forms of digital capitalism (Sharon 2016; Srnicek 2016). In turn, the rapid expansion of large corporate actors into the health sector holds the potential to fundamentally reconfigure the health ecosystem and its underlying infrastructures, fostering privatization dynamics that are possibly bound to overhaul the public nature of most European healthcare systems.

Secondly, the advent of new (corporate) actors mobilizing DHTs within different sectors leads to the creation of new health spaces within and beyond healthcare. On the one hand, the intensive resourcing of non-health-related data gathered through DHTs permits medical diagnosis to be built not merely on medical data, but to be fine-tuned with personal lifestyle data (e.g. sleep, diet, social media activity) and to be adjusted for risk scores within broader predictive models based on, for example, shopping habits, housing, water, air quality, and social network activity (Hogle 2016; Mittelstadt, Russell, and Wachter 2018; Pasquale 2015). Ever more frequently, then, types of data other than health-related ones enter the realm of healthcare institutions. This does not only lead to what has been referred to as the "lifestylization of healthcare" (Lucivero and Prainsack 2015); it also endows seemingly innocuous and mundane data with the potential to reveal detailed information on the most intimate and sensitive aspects of individuals. Con-versely, the growing possibilities for the economic valorization of health data (see also Birch et al. in this Special Issue) generate a growing interest and intensified gathering of health-related data by industries outside of the traditional medical sphere (see, e.g. Pasquale 2015). This greatly increases the potential for violating "contextual integrity" (Nissenbaum 2004) through the re-purposing of data from the biomedical domain to commercial, financial, or other social domains, which may entail significant harms for data subjects (Lupton 2018; Pasquale 2015).3 This way, DHTs render the traditional boundaries between healthcare and other societal domains increasingly instable and porous (Hogle 2016), and this in turn

questions still prevalent legal classifications of different types of data (e.g. sensitive, health-related, and anonymous) within "siloed" regulatory categories.

Finally, the data-intensive resourcing practices of DHTs enable the refinement and creation of new social categorizations and risk classifications of individuals, in healthcare as well as in other societal domains (Hogle 2016; Prainsack and Van Hoyweghen 2020; Taylor 2017). Scholars have pointed toward the performative power of DHT algorithms and data in enacting forms of social sorting,4 which may lead to the introduction of new categories of people and the further reinforcement of established beliefs about social differences (Bowker and Star 1999). The combination of different types of data is used for predictive modeling (i.e. the search for probabilistic associations to predict the likely behaviours of individuals). Within the context of healthcare, the risk scores generated by these models can, in turn, refine personalized medical diagnoses, or they can be deployed for hospital administrative purposes, such as for the evaluation of physician performance and pay (Hogle 2016). Moreover, DH data are re-purposed for risk categorization beyond the remits of healthcare (Hogle 2016; O'Doherty et al. 2016; Pasquale 2015), for instance within broader predictive models stratifying individuals into new types of risk classifications for loans (O'Neil 2017), insurance premiums (Blasimme, Vayena, and Van Hoyweghen 2019), or border security purposes (O'Doherty et al. 2016). These predictive classifications risk to worsen health disparities, for they may be deployed to generate unequal access to treatment, insurance premiums, or loans for different socio-economic groups (Ferryman and Pitcan 2018; Hogle 2016; Lupton 2018).

More broadly, harms deriving from these kinds of discriminations based on algorithmic classifications and social sorting, which may even occur on the basis of biased data or wrongful inferences (Ferryman and Pitcan 2018), can include unfair and unequal treatment, whereby, on the basis of perhaps innocuous attributes, individuals are "treated differently from other individuals similar to them in all relevant aspects" (Mittelstadt 2017, 481; for compelling case-based reviews of harms caused by algorithmic-enabled social sorting through group profiling, see; Eubanks 2018; Hogle 2016; O'Neil 2017; Pas- quale 2015). Still, these practices and their consequences are often not accounted for nor tackled in legal regimes governing DHTs.

The GDPR: misalignments and tensions with current developments in digital health

The societal reconfigurations triggered by the expansion of the digital health ecosystem and related socio-technical practices reveal tensions with the GDPR-based data governance regime. These tensions – which have been framed by some in terms of opposition (Deutscher Ethikrat 2017, 15) or outright incompatibility (Zarsky 2017) – stem from the fact that, to a great extent, regardless of the perceived "need to evolve data protection beyond the old paradigm" (Mayer-Schönberger and Padova 2016, 332), the GDPR is still predicated on standards that have their roots in past generations of data protection regulations (Kuner et al. 2012; Mantelero 2014).

In the following sections, we address relevant challenges faced by the GDPR in govern- ing the surge in big data applications and DHTs. Based on a review of data protection, legal, sociological, ethical, and policy literature, we group the shortcomings of the Regulation in four broad areas (Table 1), related to: (i) the limited scope of traditional data protection principles in accounting for shifts in modes of data processing enabled by new technological affordances and business models in the DH domain; (ii) the porosity of regulatory categories, whose neatly defined boundaries are made instable by the emergence of novel "health spaces" carved out by the use of DHTs (e.g. mHealth) and the rise of practices such as big data analytics; (iii) the pitfalls of practices of individual autonomy and control over personal data, which appear ineffective in contemporary DH environments; and (iv) the too narrow scope of the regulation toward individual and societal harms possibly occurring in such environments.

Digital health generates frictions with data protection principles

New technological affordances (such as machine learning and deep learning) (Kuner et al. 2018; Pierce 2018) and the corporate business models of DH platforms (Srnicek 2016; Van Dijck and Poell 2016 van Dijck, Poell, and de Waal 2018), have been shown to defy a number of key principles that have long since governed data protection law.5 Two principles, "purpose limitation" and "data minimization", are especially challenged by these current developments. The notion of purpose limitation is one of the mainstays of the European data protection regime, while also featuring – even more relevantly for the normative weight this carries – in one of the EU primary legal sources, the Charter of Fundamental Rights of the European Union (Art. 8(2)) (Official Journal of the European Communities 2000). Later enshrined in the GDPR, within Art. 5(1)(b), it sets forth the principle that personal data must be collected for purposes that are specified and explicit, and should not be further processed in a manner that is "incompatible" with such purposes. As Zarsky (2017) observes in his comprehensive review of big data processing in light of the GDPR, this principle is intended to allow data subjects to exercise autonomy and control over personal information (two key notions protected in the GDPR, see below). In addition, it serves to promote trust in data environments by preventing "unbridled" (Hildebrandt 2015, 212) data processing practices that may entail, as dis- cussed in the previous section, significant threats to individuals.

In a similar fashion, the GDPR upholds a data minimization requirement, which, as stated in Art. 5(1)(c), mandates that personal data processing must be adequate and limited to what is necessary in relation to the intended purposes. The data minimization principle refers to both the scope and categories of data initially collected, as well as the (limited) period for which personal data can be retained. This latter requirement is also in line with the storage limitation principle (Art. 5(1)(e), cf. also Recital 39), which allows storage of personal data only for as long as it is necessary with regard to the specific purpose for which they are processed. In line with the purpose limitation requirement, these principles are strictly related to the intention of avoiding the buildup of extensive data collections that may lead to risks of social surveillance and control (Mantelero 2014; Zarsky 2017), as well as minimizing the possibility of data breaches, whose

consequences can be hugely detrimental to data subjects (see, e.g. O'Doherty et al. 2016; Pasquale 2015, 29).

Yet, while representing the main traditional pillars of past and present data protection governance regimes, these principles appear to be in tension with DH, notably with respect to the rise of big data analytics and AI. For one thing, personal health data collected for machine learning can be put to extensive uses that cannot be specifically identified and explicitly articulated to the data subject at the time of data collection (Pierce 2018). This problem is exacerbated by the fact that, epistemically, inasmuch as machine learning algorithms "learn and develop" and hence are not necessarily directed by their programmers (Kuner et al. 2017), it can be difficult to foresee in advance the very purpose of the processing of personal data.6 In turn, this puts a strain on data retention limits, since this latter requirement substantially curbs the value that can be extracted from data.7 All these issues are further exacerbated by the typical business model of DH platforms – which is largely based on their ability to re-purpose and cross-link different flows of personal data (van Dijck, Poell, and de Waal 2018), and thus appears to collide with the application of these principles.

Aside from purpose limitation, data minimization, and storage limitation, a fourth key principle greatly challenged by DH platforms and technologies navigating big data environments is transparency. In the GDPR, the principle of transparency is enshrined in Art. 5(1)(a) (personal data are "processed lawfully, fairly and in a transparent manner in relation to the data subject"), and requires that individuals are made aware, in a form "easily accessible and easy to understand," that "personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed" (Recital 39). As such, transparency is the principle that informs the right of the individual to receive adequate information regarding the processing of personal data (Chapter III, Section 1), which acquires particular salience in the case of profiling (Art. 4(4)) and automated individual decision-making (Art 22), whose "existence," "logic involved," and "envisaged consequences" should be disclosed to the affected data subject (Art. 13(2)(f), Art. 14(2)(g); Recital 60).

Against this backdrop, the challenges posed to the principle of transparency mostly revolve around the opacity structurally involved in the undertakings of digital corporate platforms in health research and care. This potentially applies in three ways. First, opacity may refer to the proprietary regimes and corporate secrecy under which corporate platforms in DH operate (see, e.g. Kuner et al. 2017; Pasquale 2015; Powles and Hodson 2017). Secondly, opacity may pertain to the inaccessibility of algorithmic codes (and their underpinning "logic") to most but a few skilled experts, due to widespread technical illiteracy within the citizenry (Burrell 2016). Thirdly, opacity may arise, at a more fundamental level, from the very characteristics of advanced machine learning algorithms, which are not geared to human intelligibility, to the point that "the workings of machine learning algorithms can escape full understanding and interpretation by humans, even for those with specialized training, even for computer scientists" (Burrell 2016, 10). Accordingly, it is difficult to see how the transparency requirements set forth by the GDPR can be satisfied, "especially in

cases where a machine learning process involves multiple data sources, dynamic development, and elements that are opaque, whether for technological or proprietary reasons" (Kuner et al. 2017, 2).8

As a consequence of all of the above, the GDPR's key structuring principles appear mis- aligned with the surge in big data practices and DHTs, such as mHealth devices, especially those provided by large corporate actors. The tensions highlighted here could make it possible – on the one hand – that many of the provisions set forth by the GDPR are rendered "quickly irrelevant" (Zarsky 2017, 996), thus lowering the level of protection afforded to citizens in Europe. In this respect, the GDPR also contains facilitation mechanisms provided with regard to scientific research or processing for statistical purposes (see Pormeister 2017); these, among other things, enable to bypass altogether the purpose and storage limitation requirements (cf. Art. 5(b) and 5e), and can thus provide a "regulatory backdoor" to digital health platforms, effectively enabling continuous re-use and repurposing of previously collected data (see Marelli and Testa 2018; Mayer-Schönberger and Padova 2016; Pormeister 2017). Key in this regard will be how European states will differently implement these facilitation mechanisms, inasmuch as the GDPR allows for the introduction of nation-specific provisions with regard to the processing of genetic, health and biometric data (Art. 6(4)).

On the other hand, concerns have been raised that stringent enforcement of the principles encoded in the GDPR could substantially alter the unfolding of digital innovation in Europe, toward suboptimal and inefficient approaches. These could in turn hamper potential societal benefits (McMahon, Buyx, and Prainsack 2019), or severely limit innovation and the development of new digital technologies, while also doing little to improve European citizens' trust and sense of control over their personal information (Chivot 2019; Pani 2019).

DH pursuits blur GDPR's key regulatory categories

Practices in DH, especially those that are centred on inferential and predictive analytics, further undermine key categorial distinctions around which the GDPR is largely shaped – such as those demarcating non-sensitive and sensitive data, or identifiable and anonymous data.

For one thing, the distinction between non-sensitive and sensitive personal data increasingly shows signs of wear. As argued above, in light of the heightened possibility for integration and linkage between different datasets, any data, even that representing prima facie innocuous kind of information (e.g. shopping records, lifestyle habits), could conceivably convey sensitive information (e.g. health status), or lead to inferences9 or probabilistic assumptions being made, pertaining to intimate aspects of the data subject (Pasquale 2015; Prainsack and Buyx 2017, 101). This is most evident for so-called "quasi- health data," namely personal data not directly related to a health status (such as dietary, sleep, or sport habits), but otherwise capable of revealing information about a (present or future) physiological or pathological state of the individual, whose categorization under the label of sensitive data – including eligibility for the special

protections afforded to these (cf. Art 9 GDPR) – remain unclear and potentially open to challenges (Malgieri and Comandé 2017).10

As a consequence, any processing operation concerning "regular" categories of data can quickly turn into the processing of special categories of personal data, undermining the rationale for establishing this distinction (and the regulatory apparatus that revolves around it) in the first place, while also diluting the signal and message that this regulatory framework provides regarding the higher level of protection afforded to sensitive data (Zarsky 2017, 1014). Furthermore, the GDPR is ill-equipped to deal with the risks raised by inferential analytics, inasmuch as the default approach of the Regulation is geared to "focus primarily on mechanisms to manage the 'input side' of the processing" (namely data collection and processing), while conversely endowing data subjects with "far less control over how outputs [of processing, e.g. inferences,] are produced and used" (Wachter and Mittelstadt 2019, 12).

A second categorial distinction being rendered increasingly porous within DH is the one between the processing of identifiable and non-identifiable (anonymous) data, especially in fields such as genomics (Shabani and Marelli 2019). Increased circulation of different genetic datasets (notably those operated under open access models) and the possibility to crosslink them greatly raises the likelihood that bona fide anonymous data can be traced back to the individual (see, e.g. Erlich et al. 2018; Gymrek et al. 2013). Consequently, owing also to constant technological advancements, de-identified data – notably genomic data – can be said to present in most contexts residual risk of re-identification, rendering the regulatory machinery revolving around the identifiable/anonymous demarcation increasingly burdensome and ineffective for the protection of data subjects (Quinn and Quinn 2018; Shabani and Marelli 2019).

In the light of the above, scholars have contended that categorizations of these kinds look too "outdated, ineffective, and fluid" (Wachter 2019, 7) to inform regulatory developments in the post-digital era. The challenges emerging in the field of DH, especially those posed by big data analytics and the use of mHealth, mean that "data protection can no longer be statically tethered to certain categories of data and data use; rather, it must adapt to the constant recombination and re-contextualization of data" (Deutscher Ethikrat 2017, 32). This could prompt national and/or sectoral regulations aimed at tailoring the GDPR to specific processing activities (see conclusions) towards regarding any data as potentially identifiable, health-related, and sensitive (McMahon, Buyx, and Prain- sack 2019; Prainsack and Buyx 2017), thus de facto eliminating any pre-defined distinction based on the nature of the data alone.

DHTs challenge the "notice-and-consent" model

A third major pitfall of the GDPR-based governance for DH is the reliance on another of the main pillars of data protection law, which has been traditionally termed as the "informational self-determination" or "notice-and-consent" approach (see e.g. Cate 2010; Cate and Mayer-Schönberger 2013; Kuner et al. 2012; Mantelero 2014; Nissenbaum 2011; Sloan and Warner 2014).11

This approach – rooted in a distinctively liberal paradigm that conceives of the idea of privacy as an individual right to control the use of one's own data (Schwartz 1999; quoted in Cate 2010) and that

frames individuals mostly in terms of consumers (cf. Albrecht 2016a) – revolves around the idea that individuals should be endowed with adequate means to exercise their autonomy and individual choice over processing concerning their personal data. Information (notice), in this respect, is prodromal to the exercise of self-determination (consent), which in turn should not only be regarded as the expression of choice with respect to the diffusion of personal information, but also as an instrument to negotiate the latter's economic value as the data subject engages in digital transactions (Mantelero 2014, 649).

The GDPR itself, broadly conceived, is largely informed by such an approach, as most visibly revealed by the centrality of notions such as "control" (cf. e.g. Recital 7: "Natural persons should have control of their own personal data"), "consent" (Art. 6), "information," and "transparency," as well as the introduction of novel rights geared to enhance the self-determination of data subjects, such as the "right to be forgotten" (Art. 17) and the right to data portability (Art. 20).12

As widely claimed, however, the "notice-and-consent" model does not seem effective enough – per se – in mitigating the power asymmetries between data subjects and data users (see e.g. Cate 2010; Cate and Mayer-Schönberger 2013; Kuner et al. 2012; Mantelero 2014; Nissenbaum 2011; Prainsack 2017, 2019; Sloan and Warner 2014). In the domain of DH, this applies especially to commercial research carried out by direct-to-consumer genetic testing companies and related third parties (Ducharme 2018; Hayden 2012), or the increasingly diffuse, and still underregulated, mHealth technologies, such as the many "health and fitness" apps (more than 350.000) available in Google, Apple and Windows app stores (Mulder 2019).

For one thing, notices are often vague (ibid.) or inaccessible, not seldom taking the form of contracts drafted in poorly intelligible legalistic language (Hayden 2012). Even considering that the GDPR requires information provided to data subjects being easily accessible and understandable (Recital 39), a major trade-off between accessibility and the complete- ness and accuracy of this information continues to persist. This, as argued by some, actually represents an insurmountable "transparency paradox," whereby "transparency of textual meaning and transparency of practices conflict in all but rare instances" (Nissenbaum 2011, 36). In addition, individuals have shown a propensity for easily "clicking away" their privacy rights as an empty formality (Mayer-Schönberger and Padova 2016, 332) when it comes to consenting to the terms of use proposed by data controllers (see also Cate 2010). On top of that, it is debatable whether individuals are offered a real chance to freely choose to engage in virtual transactions on digital platforms, given the implicit social costs for choosing not to do so (i.e. impossibility to access services) vis- à-vis what is typically presented as an "opt-in versus opt-out" choice (Mantelero 2014; Nissenbaum 2011). In other words, in contexts in which choices appear somehow con- strained (most notably in the light of the monopolistic market dynamics and lock-in effects driving large corporate DH platforms), it is questionable whether consent amounts to anything more than "passive acquiescence" on the part of individuals (Sloan and Warner 2014).

Finally, besides presenting evident shortcomings in the safeguarding of individual data subjects, this liberal model tailored to the individual consumer unduly eschews the broader societal implications that we have recalled above deriving from the diffusion of DHTs. In a similar way, this paradigm is hardly able

to account for the "dividual" nature of genetic data (McGonigle and Shomron 2016), i.e. the fact that genetic data are partially shared with family members and next of kin. The latter could be equally harmed by misuse or unwanted uses of data, for instance related to access to consumer genomics database such as GEDMatch (Erlich et al. 2018), while at the same time being deprived of the means to prevent the processing operations leading to unwanted uses or misuse, or counter the effects deriving from them (Dove 2018b).

The GDPR maintains a narrow scope vis-à-vis harms and discriminatory practices related to processing of personal data

A final, related set of limitations of the current data protection regime concerns the narrow scope provided by the GDPR with respect to the possible individual and societal harms, such as those deriving from practices of algorithmic discrimination and social sorting, caused by the deployment of DHTs – which, as McMahon, Buyx, and Prainsack (2019) argue, results in a significantly lopsided balance of power between data controllers and data subjects.

As observed above, the GDPR maintains a narrow focus on the individual, which – however – overlooks the fact that privacy invasive practices need not target individuals as such; rather, the mere clustering and classification of individuals into algorithmically constructed groups according to their behaviour, preferences, and other characteristics is sufficient to drive decisions that may potentially carry harmful consequences for members of the ad hoc constructed group (Gutwirth and Hildebrandt 2008; Mittelstadt 2017). Moreover, harms can be exacerbated by the fact that individuals are largely unaware of being classified in a certain group, and thus do not have the opportunity to take appropriate counter actions (such as exercising the set of rights the GDPR bestows upon them). Additionally, while patterns and correlations used to group individuals are often- times de facto functionally equivalent to personal identifiers (e.g. name, address), and sometimes even to sensitive protected attributes (e.g. ethnicity), it remains questionable whether they are afforded comparable status under the GDPR (Mittelstadt 2017, 479), also owing to misalignments between anti-discrimination and data protection legislations (Drechsler and Benito Sánchez 2018). Importantly, even though individuals have the right under the GDPR to be informed of the existence, logic, and potential consequences (Art. 13(2)(f), Recital 71) of automated decision-making processes, as well as to obtain human intervention, and contest the decision taken (Art. 22(3)), these rights appear to have minimal effects in practice, as they are somehow ill-defined and can be easily sidestepped by data controllers (Pormeister 2017; Mittelstadt and Floridi 2016; Wachter, Mittelstadt, and Floridi 2017; Zarsky 2017).

In addition, the GDPR has been observed to maintain an (insufficiently) narrow approach to preemptively address, and adequately compensate data subjects for, possible harms and discriminations of different sorts deriving from the use of big (health) data. On the one side, given the pervasive nature of big data, potential harms caused by big data processing activities may fall outside the remit of the legislation.13 At the same time, given the "multiple" nature of digital data (that is, the fact that it can be processed in

different places at the same time; see Prainsack 2019), the combinatorial possibilities among different data types, as well as the opacity of digital health platforms and algorithms (Powles and Hodson 2017), it may be difficult to trace potential harms back to a clearly delineated chain of causality, such as the one required for traditional data protec- tion based legal remedies to apply. In both cases, data subjects would be left high and dry from a legal perspective to assert and safeguard their rights and interests. Moreover, it remains to be seen whether the increased penalties entailed by the GDPR (cf. Art. 83) will be sufficient to act as deterrent toward data misuse and abuse, especially in the light of the two points just mentioned (McMahon, Buyx, and Prainsack 2019).

Conclusions

With the entrance into effect of the GDPR in 2018, the EU laid down the foundational basis for a new harmonized data protection framework in the continent. In its concrete implementation, the GDPR has been predicted not only to lay the basis for a new regime of data governance in Europe, but also to have an "immense" impact beyond (Dove 2018a, 1013), thus serving as the "global gold standard for every new innovation, for consumer trust in digital technologies and for an entry point to the growth opportunities of an emerging digital market" (Albrecht 2016b, 288).

Yet, moving beyond a narrow legal framework and taking on a broader perspective on the sustainability of the digital health ecosystem, i.e. on the promotion of "mutually beneficial interactions" between DHTs and society writ large (Taylor and Purtova 2019, 1), one is confronted with questions over the ability of the GDPR to effectively steer data governance toward such aim. In this article, in particular, we drew upon a growing corpus of legal, socio-political, ethical, and policy studies to review key misalignments and tensions between the GDPR and the practices revolving around DHTs. In so doing, we pointed to four broad areas related to the limited scope of traditional data protection principles vis-à- vis emerging big data practices, the blurring of key regulatory categories, the pitfalls of the notice-and-consent model, and the narrow scope of the regulation towards harms and discriminations deriving from data processing operations.

We argue that these issues are revealing of the underlying difficulty of the GDPR-based data governance framework to adequately recognize the "constitutional" reach (Jasanoff 2003) of contemporary DHTs – that is, the role these technologies and their attending socio-economic practices play in reshaping social structures and fundamental normative tenets (such as the meaning of constructs like "individual autonomy") in contemporary societies. New types of actors, in the guise of large consumer technology corporations, make their appearance within the domain of health research and care, rendering the latter prone to the dynamics that characterize emerging forms of digital capitalism. All the while, the boundary between the health domain and other societal domains gives way to new "health data protection grey zones" (Lievevrouw and Van Hoyweghen 2019), where distinctions between different data types (e.g. health vs.

lifestyle, sensitive vs. non-sensitive), and data uses (medical vs. commercial), become increasingly blurred. In turn, novel data processing activities perform new forms of social sorting and social classifications, to the potential detriment of relevant parts of the population. All these issues are for the most part forgone by the GDPR – owing perhaps also to the disruptions that more radical departures from the previous legislation could have caused in day-to-day legal practice.

Scholars have put forward a number of regulatory tools to adjust or complement the current legal framework of the GDPR. Some have proposed to move away from the still dominant informational self-determination approach to the implementation of a use- based framework. The latter would focus less – or at least not exclusively – on individual consent, and would move upstream the assessment of potential harms deriving from Big Data processing (cf. e.g. Cate and Mayer-Schönberger 2013). Largely in a similar vein, another strand of scholarship has insisted on imbuing data governance with solidarity- based frameworks, tailored to gear up forms of collective, rather than individual, control and oversight (cf. e.g. Prainsack 2017). Still other proposals, in line with the former, suggest to move beyond the "risk" framing of the GDPR and establish harm miti- gation bodies, directed at both addressing the power asymmetries inherently raised by big data processing and provide mechanisms in support of individuals harmed by such processing operations (cf. e.g. McMahon, Buyx, and Prainsack 2019). The goal of establishing a sustainable health ecosystem is best tackled, according to some others, by resorting to the analytical framework of the "commons" (cf. e.g. Taylor and Purtova 2019).

In the final analysis, how can this growing body of analyses concretely inform policy- making? We suggest two possible viable paths. First, the date of May 25, 2020, when the European Commission is due to submit a report on the evaluation and review of the GDPR (pursuant to Art. 97 GDPR) is approaching. This (limited) timespan can serve the purpose of taking stock of the current workings and shortcomings of the regulation and plan, where needed, more effective legislative remedies. In the meantime, a number of policy initiatives at both the European and national level in member states such as Italy, Norway, and Poland, to name but a few, are setting Ministerial Guidelines and Codes of Conduct (pursuant to Art. 40 GDPR) for tailoring the application of the Regulation to the context of health research and care. Likewise, these soft law instruments have the potential to be informed by ongoing critical reflections on data governance, so as to mitigate some of the exposed shortcomings of the Regulation and move toward the creation of a more sustainable digital health ecosystem. At any rate, we consider it paramount that the lessons learned through the concerted efforts of legal, data protection, policy, sociological, and ethical scholarship is not dispersed, but can concretely provide the foundation for policy responses rooted in effective and socially robust governance mechanisms.

Notes

1. As a "Regulation," the GDPR achieves regulatory harmonization inasmuch as it is immediately applicable upon its entry into effect across all European member states. By contrast, a "Directive"

does not have direct effect as such; to become effective, it needs to be transposed in member states' national law. However, it should be noted that the GDPR still allows member states to introduce further specific provisions – for instance with regard to the processing of health, genetic, and biometric data (Art. 9(4) GDPR).

2. Lupton defines DHTs as "technologies directed at delivering healthcare, providing information to lay people and helping them share their experiences of health and illness, training and educating healthcare professionals, helping people with chronic illness to engage in self- care and encouraging others to engage in activities to promote their health and wellbeing and avoid illness." (Lupton 2018, 1).
3. Following the definition advanced by Redden and Brand in their Data Harm Record drafted within the Data Justice Lab at Cardiff University (https://datajusticelab.org/data-harm- record/), data harms are "the adverse effects caused by uses of data that may impair, injure, or set back a person, entity or society's interests." At the same time, as Price and Cohen (2019, 40) contend, deontological – as opposed to consequentialist – harms may arise even in absence of any "material consequences for the individual or if the individual does not even know."
4. Social sorting can be defined as "the use of information to create profiles that may have consequences for the way individuals are viewed by payers, by consumer marketing groups, and others" (Hogle 2016, 423).
5. The codification of data protection principles (such as those of "collection limitation," "purpose specification," "use limitation") owes especially to the draft of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by the OECD (OECD 1980), as well as other early normative documents (such as the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data) (Council of Europe 1981) that were closely aligned with the OECD principles (for a discussion on this, see Lowrance 2012).
6. For instance, a dataset containing genetic and health data collected for medical purposes, processed by (machine learning) algorithmic models geared to identify correlations between genetic and/or phenotypic features of the individuals and health outcomes or drug response, may well reveal other relevant correlations (e.g. regarding a different disease from the one initially targeted) that could not be explicitly foreseen at the time of data collection. Or, input data related to a particular patient may be relevant to other uses beyond the purpose of care for that particular patient (Pierce 2018) – which, as observed, may be of concern in particular if data travel outside the regulated healthcare domain.
7. At their core, these tensions boil down to the fact that big data practices bring about a fundamental change in the way scientific and economic value is extracted from datasets. Whereas in the past the value of data "was captured by collecting and using it once for a concrete purpose, with big data the latent value of data is unclear at the time of data collection and can only be fully reaped as the data is being reused over and over again for different purposes" (Mayer- Schönberger and

Padova 2016, 319–320). This shift creates consequently a strong (epistemic as well as economic) incentive in "opportunistic" rather than "purposeful" collection of personal data, as well as repeated and combinatorial use of the datasets gathered (ibid.).

8. In addition, it is important to note that, in particular with respect to automated individual decision-making, lack of proper information can, in turn, impede the full exercise of individual rights, such as those of obtaining human intervention on the part of the controller or con- testing the automated decision (Art. 22(3) GDPR).
9. Inferences can be defined in this context as "information relating to an identified or identifiable natural person created through deduction or reasoning rather than mere observation or collection from the data subject" (Wachter and Mittelstadt 2019, 13). Inferences can be "high risk" if they are "privacy-invasive or harmful to reputation, or have a high likelihood of being so in the future, and have low verifiability in the sense of being predictive or opinion-based" (ibid.). In turn, both kinds of inferences have been said to be "'economy class' data in the GDPR," devoid of the protection afforded to the processing of other types of data, also in the light of possible conflicts arising with the protection of commercial interests attached to their underlying models and algorithms (Wachter and Mittelstadt 2019, 2).
10. However, we should note in this regard the strict approach taken by the Court of Justice of the European Union (CJEU) in enforcing a more stringent regime to cases where potential proxies for sensitive data have been used (cf. Drechsler and Benito Sánchez 2018, who also recall Opinion 1/15 of 26 July 2017 of the CJEU on the EU-Canada Passenger Name Record Agreement, which considered special requests such as food preferences on planes akin to sensitive information).
11. The "notice and consent" approach, including its underlying logic, has also been labelled as the "individual control" approach (Prainsack 2019) and the "consent or anonymize" approach (see e.g. Mostert et al. 2016; Dove 2018a), whereby anonymization is posited as the sole possible alternative to obtaining consent from data subjects for personal data processing, most notably within biomedical research.
12. It should be noted, however, that a movement that (partially) counter the overall direction taken by the GDPR in upholding the "notice and consent" model predicated on an informed, freely given, and specific consent (see e.g. Mantelero 2014, 645), is its support of broad consent for scientific research whenever the criterion of specific consent for specific research use at the moment of data collection proves impossible to satisfy (Recital 33; Marelli and Testa 2018; cf. also Art. 29 WP 2018).
13. For example, as McMahon, Buyx, and Prainsack (2019, 9) argue, "a person who is harmed by a predictive analytics system that makes probabilistic inferences regarding an undesirable trait on the basis of generic information about her – such as the postcode she lives in – does not have access to legal remedies if the data that was used to make these inferences is not her own personal data."

Acknowledgement

The authors would like to thank Barbara Prainsack and the anonymous reviewers for their insightful and constructive comments that helped improving the argument and flow of the article.

Disclosure statement

No potential conflict of interest was reported by the author(s). Funding

This work was supported by the European Union's Horizon 2020 research and innovation program, under the Marie Sklodowska-Curie grant agreement number 753531 (LM), and the Research Foundation Flanders (FWO), under the Odysseus Project 'Postgenomic Solidarity. European Life Insurance in the Era of Personalised Medicine' [grant number 3H140131, IVH] and the PhD Fellowship Fundamental Research [grant number 11C8520N, EL].

Notes on contributors

Luca Marelli (PhD, 2016) is a Marie Skłodowska-Curie Fellow with the Life Sciences & Society Lab at the Centre for Sociological Research (KU Leuven). He also holds appointments as a Visiting Research Fellow at the Department of Experimental Oncology (European Institute of Oncology, Milan) and an Adjunct Professor of Bioethics at the Department of Medical Biotechnologies and Translational Medicine (University of Milan). His main research activities, at the intersection of Science & Technology Studies (STS), data governance and biomedical research policy, focus on the ethical, legal, and social aspects of contemporary data-intensive biomedicine in the European Union. As the Scientific Secretary of the ACC GDPR Committee, established under the aegis of the Italian Ministry of Health, Marelli is presently involved in devising binding guidelines for the implementation of national and European legislation on data protection for the processing activities of Italian research hospitals (IRCCS, Istituti di Ricovero e Cura a Carattere Scientifico).

Elisa Lievevrouw is an FWO PhD Fellow with the Life Sciences & Society Lab at the Centre for Sociological Research (KU Leuven). Her doctoral research, at the intersection between Foucauldian, Science & Technology, and socio-legal studies, focuses on the social aspects of digital health policy- making in the United States and the European Union.

Ine Van Hoyweghen is a Research Professor at the Centre for Sociological Research (KU Leuven) where she directs the Life Sciences & Society Lab. She is a leading and internationally renowned researcher in sociology of biomedicine, science and technology studies (STS), and governance of health care innovation. Her main research activities concentrate on the ethical, legal and social implications of biomedical innovations (genomics, digital health, personalized medicine, artificial intelligence). Van Hoyweghen is the author of many books, including Risks in the Making. Travels in Life Insurance and Genetics (Amsterdam University Press, 2007), Making Global Health Care Innovation Work. Standardization and Localization

(2014, Palgrave, with Engel, N. & Krumeich, A.), Citizen Science (2019, with Gijsel, L. & Huyse, T.) and Shifting Solidarities. Trends and Developments in European Societies (2020, Palgrave, with Pulignano, V. & Meyers, G.).

References

Albrecht, J. 2016a. "Conclusion of the EU Data Protection Reform." last accessed January 10 2020. https://www.janalbrecht.eu/2016/04/2016-04-13-conclusion-of-the-eu-data-protection-reform/.

Albrecht, J. 2016b. "How the GDPR Will Change the World." *European Data Protection Law Review* 2: 287–289.

Andrejevic, M. 2014. "The Big Data Divide." *International Journal of Communication* 8: 1673–1689. Article 29 Data Protection

Working Party. 2018. Guidelines on Consent under Regulation 2016/679, WP259. Last accessed January 10 2020. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Australian Digital Health Agency. 2018. *Australia's National Digital Health Strategy. Safe, Seamless and Secure: Evolving Health and Care to Meet the Needs of Modern Australia*. Accessed 10th of December 2019. https://conversation.digitalhealth.gov.au/sites/default/files/adha-strategy-doc- 2ndaug_0_1.pdf [last accessed January 10 2020].

Blasimme, A., E. Vayena, and I. Van Hoyweghen. 2019. "Big Data, Precision Medicine and Private Insurance: A Delicate Balancing Act." *Big Data & Society* 6 (1).

Bowker, G. C., and S. L. Star. 1999. *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT press.

Boyd, D., and K. Crawford. 2012. "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon." *Information, Communication & Society* 15 (5): 662–679.

Burrell, J. 2016. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." Big Data & Society 3 (1): 2053951715622512.

Cate, F. 2010. "Protecting Privacy in Health Research: The Limits of Individual Choice." *California Law Review* 98 (6): 1765.

Cate, F. H., and V. Mayer-Schönberger. 2013. "Notice and Consent in a World of Big Data." *International Data Privacy Law* 3 (2): 67–73.

Chivot, E. 2019. "One Year on, GDPR Needs a Reality Check." *Financial Times*, June 30 2019. Last accessed January 10 2020. https://www.ft.com/content/26ee4f7c-982d-11e9-98b9-e38c177b152f.

Council of Europe. 1981. *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*. European Treaty Series No. 108. https://www.coe.int/en/web/ conventions/full-list/-/conventions/rms/0900001680078b37.

Deutscher Ethikrat. 2017. *Big Data and Health – Data Sovereignty as the Shaping of Informational Freedom*. Opinion. Executive Summary & Recommendations. Last accessed January 10 2020. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data- and-health-summary.pdf.

Dove, E. S. 2018a. "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era." *The Journal of Law, Medicine & Ethics* 46 (4): 1013–1030.

Dove, E. S. 2018b. "Collection and Protection of Genomic Data." In *Routledge Handbook of Genomics, Health and Society*, edited by E. S. Dove, 161–168. London: Routledge.

Drechsler, L., and J. C. Benito Sánchez. 2018. "The Price Is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms." *European Journal of Law and Technology* 9 (3). http://ejlt.org/article/view/631/854.

Ducharme, J. 2018. "A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?" *Time Magazine*, July 2018.

Erlich, Y., T. Shor, I. Pe'Er, and S. Carmi. 2018. "Identity Inference of Genomic Data Using Long-Range Familial Searches." *Science (New York, N.Y.)* 362 (6415): 690–694.

Eubanks, V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*. New York: St Martin's Press.

European Commission. 2014a. *Commission Staff Working Document on the Existing EU Legal Framework Applicable to Lifestyle And Wellbeing Apps Accompanying the Document GREEN PAPER on Mobile Health ("mHealth")*. Last accessed January 10 2020. https://op.europa.eu/ en/publication-detail/-/publication/8dcf22a2-c091-11e3-86f9-01aa75ed71a1/language-en.

European Commission. 2014b. *Green Paper on Mobile Health ("mHealth")*. https://ec.europa.eu/ digital-single-market/en/news/green-paper-mobile-health-mhealth.

European Commission. 2018. *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Enabling the Digital Transformation of Health and Care in the Digital Single Market; Empowering Citizens and Building a Healthier Society,* COM(2018)33. https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering.

Farr, C. 2018. "Google Sister-company Verily is Plotting a Move into a Fast- growing Corner of the Health Insurance Industry." *CNBC*. February 2018. Last accessed January 10 2020. https://www. cnbc.com/2018/02/27/alphabet-verily-health-insurance-care-management.html.

FDA. 2013. *Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff*. Last accessed January 10 2020. https://www.fda.gov/media/80958/download.

FDA. 2019. "Digital Health." Last accessed January 10 2020. https://www.fda.gov/medical-devices/ digital-health.

Federal Ministry of Health. 2019. "Digital Healthcare Act (DVG)". Last accessed January 10 2020. https://www.bundesgesundheitsministerium.de/digital-healthcare-act.html.

Ferryman, K., and M. Pitcan. 2018. *Fairness in Precision Medicine*, Data&Society. Last accessed January 10 2020. https://datasociety.net/wp-content/uploads/2018/02/Data.Society.Fairness.In_.Precision.Medicine.Feb2018.FINAL-2.26.18.pdf.

Gottlieb, S. 2018. "Transforming FDA's Approach to Digital Health." Academy Health's 2018 Health Datapalooza. Washington D.C. Last accessed January 10 2020. https://www.fda.gov/ news-events/speeches-fda-officials/transforming-fdas-approach-digital-health-04262018.

Gutwirth, S., and M. Hildebrandt. 2008. *Profiling the European Citizen: Cross-Disciplinary Perspectives*. New York: Springer.

Gymrek, M., A. L. McGuire, D. Golan, E. Halperin, and Y. Erlich. 2013. "Identifying Personal Genomes by Surname Inference." *Science (New York, N.Y.)* 339 (6117): 321–324.

Haute Autorité de Santé. 2016. *Good Practice Guidelines on Health Apps and Smart Devices (Mobile Health or mHealth)*. https://www.has-sante.fr/upload/docs/application/pdf/201703/dir1/good_practice_guidelines_on_health_apps_and_smart_devices_mobile_health_or_mhealth.pdf.

Hayden, E. 2012. "Informed Consent: A Broken Contract." *Nature* 486 (7403): 312.

Hildebrandt, M. 2015. "Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology." *European Data Protection Law Review* 1 (2): 157–159.

Hoeyer, K. 2016. "Denmark at a Crossroad? Intensified Data Sourcing in a Research Radical Country." *The Ethics of Biomedical Big Data* 29: 73–93.

Hogle, L. F. 2016. "Data-intensive Resourcing in Healthcare." *BioSocieties* 11 (3): 372–393.

IGES Institute. 2016. *Digital Healthcare Products: Leveraging Opportunities – Developing Safe Routes to Market*. Berlin. Last accessed January 10 2020. https://www.iges.com/e6/e1621/e10211/e13470/e15278/e15279/e15281/attr_objs15282/IGES_Publication_Digital_healthcare_products_WEB_eng.pdf.

IMI. 2014. *The Right Prevention and Treatment for the Right Patient at the Right Time. Strategic Research Agenda for Innovative Medicines Initiative 2*. Last accessed January 10 2020. https://www.ffg.at/sites/default/files/imi2_sra_march2014.pdf.

Jasanoff, S. 2003. "In a Constitutional Moment: Science and Social Order at the Millennium." In *Social Studies of Science and Technology: Looking Back, Ahead*, edited by Bernward Joerges, Helga Nowotny, 155–180. Dordrecht: Springer.

Kumar, Sudhesh. 2019. *Capitalising on Japan's Digital Healthcare Economy During this Era of Aging Societies*. HIMMS Europe. Last accessed January 10 2020. https://www.himss.eu/content/ capitalising-japans-digital-healthcare-economy-during-era-aging-societies.

Kuner, Christopher, Fred H. Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain, Dan Jerker B. Svantesson, et al. 2018. "Expanding the Artificial Intelligence-data Protection Debate." 289–292.

Kuner, C., F. H. Cate, C. Millard, and D. J. B. Svantesson. 2012. "The Challenge of 'Big Data' for Data Protection." *International Data Privacy Law* 2 (2): 47–49.

Kuner, C., D. J. B. Svantesson, F. H. Cate, O. Lynskey, and C. Millard. 2017. "Machine Learning with Personal Data: Is Data Protection law Smart Enough to Meet the Challenge?" *International Data Privacy Law* 7 (1): 1–2.

Lievevrouw, E., and I. Van Hoyweghen. 2019. "The Social Implications of Digital Health Technology." In *Mobile Health Revolution in Healthcare: Are We Ready?*, 43–48. Metaforum KU Leuven. https://www.kuleuven.be/metaforum/docs/pdf/wg_58_e.pdf.

Lowrance, William W. 2012. *Privacy, Confidentiality, and Health Research. Cambridge Bioethics and Law*. Cambridge: Cambridge University Press.

Lucivero, F., and B. Prainsack. 2015. "The Lifestylisation of Healthcare? 'Consumer Genomics' and Mobile Health as Technologies for Healthy Lifestyle." *Applied & Translational Genomics* 4: 44–49.

Lupton, D. 2018. *Digital Health: Critical and Cross-Disciplinary Perspectives (Critical Approaches to Health)*. New York: Routledge.

Mager, A. 2017. "Search Engine Imaginary: Visions and Values in the Co-Production of Search Technology and Europe." *Social Studies of Science* 47 (2): 240–262.

Malgieri, G., and G. Comandé. 2017. "Sensitive-by-distance: Quasi-Health Data in the Algorithmic era." *Information & Communications Technology Law* 26 (3): 229–249.

Mantelero, A. 2014. "The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics." *Computer Law & Security Review: The International Journal of Technology Law and Practice* 30 (6): 643–660.

Marelli, L., and G. Testa. 2018. "Scrutinizing the EU General Data Protection Regulation." *Science* 360 (6388): 496–498.

Mayer-Schönberger, V., and Y. Padova. 2016. "Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation." *The Columbia Science & Technology Law Review* 17 (1) (Spring): 315–335.

McGonigle, I., and N. Shomron. 2016. "Privacy, Anonymity and Subjectivity in Genomic Research." *Genetics Research* 98: e2.

McMahon, A., A. Buyx, and B. Prainsack. 2019. "Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond." *Medical law Review*, 1–28.

Medicines & Healthcare products Regulatory Agency. 2014. *Guidance: Medical Device Stand-alone Software Including Apps (including IVDMDs)*. Last accessed January 10 2020. https://www.gov.uk/government/publications/medical-devices-software-applications-apps.

Ministry of Health Singapore. 2019. "Licensing Experimentation and Adaptation Programme (LEAP) – A Regulatory Sandbox". Last accessed January 10 2020. https://www.moh.gov.sg/ our-healthcare-system/licensing-experimentation-and-adaptation-programme-(leap)—a-moh- regulatory-sandbox.

Mittelstadt, B. 2017. "From Individual to Group Privacy in Big Data Analytics." *Philosophy & Technology* 30 (4): 475–494.

Mittelstadt, B., and L. Floridi. 2016. "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts." *Science and Engineering Ethics* 22 (2): 303–341.

Mittelstadt, B., C. Russell, and S. Wachter. 2018. "Explaining Explanations in AI." *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 279–288.

Mostert, M., A. L. Bredenoord, M. C. Biesaart, and J. J. Van Delden. 2016. "Big Data in Medical Research and EU Data Protection law: Challenges to the Consent or Anonymise Approach." *European Journal of Human Genetics* 24 (7): 956–960.

Mulder, T. 2019. "Health Apps, Their Privacy Policies and the GDPR." *European Journal of Law and Technology* 10 (1). http://ejlt.org/article/view/667/897.

National Institute for Health and Care Excellence. 2019. *Evidence Standards Framework for Digital Health Technologies*. UK, National Institute for Health and Care Excellence (NICE). Last accessed January 10 2020. https://www.nice.org.uk/about/what-we-do/our-programmes/ evidence-standards-framework-for-digital-health-technologies.

Nissenbaum, H. 2004. "Privacy as Contextual Integrity. (Symposium: Technology, Values, and the Justice System)." *Washington Law Review* 79 (1): 119–157.

Nissenbaum, H. 2011. "A Contextual Approach to Privacy Online." *Daedalus* 140 (4): 32–48.

O'Doherty, K. C., E. Christofides, J. Yen, H. B. Bentzen, W. Burke, N. Hallowell, B. A. Koenig, and D. J. Willison. 2016. "If You Build It, They Will Come: Unintended Future Uses of Organised Health Data Collections." *BMC Medical Ethics* 17 (1): 54.

OECD. 1980. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Official Journal of the European Communities. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.* Last accessed January 10 2020. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

Official Journal of the European Communities. 2000. *Charter of Fundamental Rights of the European Union (2000/C 365/01).* Last accessed January 10 2020. https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Official Journal of the European Union. 2016. *Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).* Last accessed January 10 2020. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Official Journal of the European Union. 2017a. *Regulation (EU) 2017/745 of the European Parliament and the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/ EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC.* Last accessed January 10 2020. https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745.

Official Journal of the European Union. 2017b. *Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in Vitro Diagnostic Medical Devices and Repealing Directive 98/79/EC and Commission Decision 2010/227/EU.* Last accessed January 10 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0746.

O'Neil, C. 2017. *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy.* New York: Penguin Books.

Ordish, J., M. Hannah, and H. Allison. 2019. *Algorithms as Medical Devices.* PHG Foundation. Last accessed January 10 2020. https://www.phgfoundation.org/report/algorithms-as-medical- devices.

Pani, L. 2019. "Setting the Stage. Digital Medicine and the Brain." Slides presented at the IMI stakeholder Forum 2019 on Brain health and disease in the digital era – 2020 & beyond, Brussels, June 12.

Pasquale, F. 2015. *The Black Box Society. The Secret Algorithms That Control Money and Information.* Cambridge, MA: Harvard University Press.

Petersen, A. 2019. *Digital Health and Technological Promise: A Sociological Inquiry.* New York: Routledge.

Pierce, R. 2018. "Machine Learning for Diagnosis and Treatment: Gymnastics for the GDPR." *European Data Protection Law Review* 4 (3): 333–343.

Pormeister, K. 2017. "Genetic Data and the Research Exemption: is the GDPR Going too Far?" *International Data Privacy Law* 7 (2): 137–146.

Powles, J., and H. Hodson. 2017. "Google DeepMind and Healthcare in an Age of Algorithms." *Health and Technology* 7 (4): 351–367.

Prainsack, B. 2017. "Research for Personalised Medicine: Time for Solidarity." *Medicine and Law* 36 (1): 87–98.

Prainsack, B. 2019. "Logged Out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons." *Big Data Society* 6: 1.

Prainsack, B., and A. Buyx. 2017. *Solidarity in Biomedicine and Beyond.* Cambridge: Cambridge University Press.

Prainsack, B., and I. Van Hoyweghen. 2020. "Shifting Solidarities: Personalisation in Insurance and Medicine." In *Shifting Solidarities. Trends and Developments in European Societies*, edited by I. Van Hoyweghen, V. Pulignano, and G. Meyers. New York: Palgrave Macmillan.

Price, W. N., and I. G. Cohen. 2019. "Privacy in the age of medical big data." *Nature Medicine* 25 (1): 37–43.

Quinn, P., and L. Quinn. 2018. "Big Genetic Data and Its Big Data Protection Challenges." *Computer Law & Security Review* 34: 1000–1018.

Saunders, G., M. Baudis, R. Becker, S. Beltran, C. Béroud, E. Birney, C. Brooksbank, et al. 2019. "Leveraging European Infrastructures to Access 1 Million Human Genomes by 2022." *Nature Reviews Genetics* 20: 693–701.

Shabani, M., and L. Marelli. 2019. "Re-Identifiability of Genomic Data and the GDPR." *EMBO Reports* 20: 6.

Sharon, T. 2016. "The Googlization of Health Research: From Disruptive Innovation to Disruptive Ethics." *Personalized Medicine* 13 (6): 563–574.

Sharon, T., and F. Lucivero. 2019. "Introduction to the Special Theme: The Expansion of the Health Data Ecosystem – Rethinking Data Ethics and Governance." *Big Data & Society* 6 (2): 1–5.

Sloan, R. H., and R. Warner. 2014. "Beyond Notice and Choice: Privacy, Norms, and Consent." *The Journal of High Technology Law* 14 (2): 370.

Srnicek, N. 2016. *Platform Capitalism*. Oxford: Polity Press.

Taylor, L. 2017. "What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society* 4: 2.

Taylor, L., and N. Purtova. 2019. "What is Responsible and Sustainable Data Science?" *Big Data & Society* 6 (2): 2053951719858114.

Van Dijck, J., and T. Poell. 2016. "Understanding the Promises and Premises of Online Health Platforms." *Big Data & Society* 3 (1): 2053951716654173.

van Dijck, J., T. Poell, and M. de Waal. 2018. *The Platform Society. Public Values in a Connective World*. New York: Oxford University Press Inc.

Vayena, E., T. Haeusermann, A. Adjekum, and A. Blasimme. 2018. "Digital Health: Meeting the Ethical and Policy Challenges." *Swiss Medical Weekly* 148 (3-4): w14571–w14571.

Wachter, S. 2019. "Data Protection in the Age of Big Data." *Nature Electronics* 2 (1): 6–7.

Wachter, S., and B. Mittelstadt. 2019. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. (Artificial Intelligence) (Survey: Privacy, Data, and Business)." *Columbia Business Law Review* 2019 (2): 494–620.

Wachter, S., B. Mittelstadt, and L. Floridi. 2017. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7 (2): 76–99.

WHO. 2019a. *WHO Guideline: Recommendations on Digital Interventions for Health System Strenghtening*. Geneva: WHO. Last accessed January 10 2020. https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/.

WHO. 2019b. *The Health Data Ecosystem and Big Data*. Accessed September 2019, last accessed January 10 2020. https://www.who.int/ehealth/resources/ecosystem/en/.

WHO Director-General. 2017. *mHealth: Use of Appropriate Digital Technologies for Public Health*. Geneva: World Health Organization. . Last accessed January 10 2020. https://apps.who.int/iris/handle/10665/274134.

Wingfield, N., K. Thomas, and R. Abelson. 2018. *"Amazon, Berkshire Hathaway and JPMorgan Team Up to Try to Disrupt Health Care."* The New York Times, January 30. Last accessed January 10 2020. http://www.nytimes.com/2018/01/30/technology/amazon-berkshire-hathaway-jpmorgan- health-care.html.

Zarsky, T. 2017. "Incompatible: The GDPR in the Age of Big Data." *Seton Hall Law Review* 47 (4): 995–1020.