Health Data Privacy under the GDPR

The growth of data-collecting goods and services, such as ehealth and mhealth apps, smart watches, mobile fitness and dieting apps, electronic skin and ingestible tech, combined with recent technological developments such as increased capacity of data storage, artificial intelligence and smart algorithms, has spawned a big data revolution that has reshaped how we understand and approach health data. Recently, the COVID-19 pandemic has foregrounded a variety of data privacy issues. The collection, storage, sharing and analysis of health- related data raises major legal and ethical questions relating to privacy, data protection, profiling, discrimination, surveillance, personal autonomy and dignity.

This book examines health privacy questions in light of the General Data Protection Regulation (GDPR) and the general data privacy legal framework of the European Union (EU). The GDPR is a complex and evolving body of law that aims to deal with several technological and societal health data privacy problems, while safeguarding public health interests and addressing its internal gaps and uncertainties. The book answers a diverse range of questions including: What role can the GDPR play in regulating health surveillance and big (health) data analytics? Can it catch up with Internet-age developments? Are the solutions to the challenges posed by big health data to be found in the law? Does the GDPR provide adequate tools and mechanisms to ensure public health objectives and the effective protection of privacy? How does the GDPR deal with data that concern children's health and academic research?

By analysing a number of diverse questions concerning big health data under the GDPR from various perspectives, this book will appeal to those interested in privacy, data protection, big data, health sciences, information technology, the GDPR, EU and human rights law.

Dr. Maria Tzanou is Senior Lecturer in Law at Keele University, United Kingdom.

Routledge Research in the Law of Emerging Technologies

Biometrics, Surveillance and the Law
Societies of Restricted Access, Discipline and Control
Sara M. Smyth

Artificial Intelligence, Healthcare, and the Law
Regulating Automation in Personal Care
Eduard Fosch-Villaronga

Health Data Privacy under the GDPR
Big Data Challenges and Regulatory Responses
Edited by Maria Tzanou

For more information about this series, please visit: www.routledge.com/Routledge-Research-in-the-Law-of-Emerging-Technologies/book-series/LAWTECHNOLOGY

Health Data Privacy under the GDPR

Big Data Challenges and Regulatory Responses

Edited by Maria Tzanou

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2021
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

Library of Congress Cataloging-in-Publication Data
A catalog record for this book has been requested

ISBN: 978-0-367-07714-3 (hbk)
ISBN: 978-0-429-02224-1 (ebk)

Typeset in Bembo
by Apex CoVantage, LLC

To Alexis, Daphne and Raul

Contents

Preface

The big data revolution has brought forward a tectonic shift in the ways we understand and approach data. Big data is both about the ability to gather and store huge amounts of data and to analyse these to discover unknown patterns and correlations. Such patterns are ultimately expected to lead to 'better and more informed decisions'[1] in healthcare, medical and scientific research, advertising, policing, surveillance and a whole range of businesses and organisations that develop products and services based on the crunching of data.

The recent COVID-19 pandemic is not only an unprecedented global health emergency; it has also foregrounded a variety of data privacy issues. Billions of people are required to comply with social distancing rules and endure mass digital surveillance of their location, communications and movements. Governments around the globe implement programmes for mobile data tracking, confidential health data are shared with private companies to produce pandemic models,[2] apps are developed to record and trace individuals' personal contact with others,[3] CCTV networks are equipped with facial recognition to monitor individuals' movements, permission regimes are deployed to authorise individuals to go outside and drones are used to enforce social isolation rules.[4]

Over the years, while big data has promised to 'improve preventive medicine' and 'keep us away from hospitals',[5] we are more and more often faced with media stories about sex toys that 'talk data';[6] spying vibrators;[7] a women's fertility app funded by anti-abortion campaigners;[8] the harvesting of 50 million Facebook profiles of US voters by Cambridge Analytica 'to build a powerful software program to predict and influence choices at the ballot box'[9] and so on.

How can the law protect us from such egregious data misuses? What are the appropriate legal solutions to address health data surveillance? Are laws regulating 'personal data' appropriate and fit-for-purpose to regulate big health data as well? These are pertinent questions that legislators worldwide are pondering.

To stay ahead of the technological developments curve, European Union (EU) institutions negotiated and adopted 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 (the 'General Data Protection Regulation' or 'GDPR').[10] The GDPR entered into force in all EU Member States (MS) on

25 May 2018 with the aim to modernise data protection rules to 'catch up with the digital age'[11] and ensure that 'the EU remains the global gold standard in the protection of personal data'.[12] Indeed, the EU data protection legislative framework is considered as 'a cornerstone of the European human-centric approach to innovation'.[13]

The GDPR has successfully[14] completed its first years of life, but questions arise about its capabilities, functionalities and potential. What role can it play in regulating health surveillance and big (health) data analytics? Can it catch up with Internet-age developments? Can it effectively deal with the 'digital breadcrumbs'[15] that our everyday activities and our own bodies drop online every second?

In ancient Greek mythology, Sisyphos, the king of Ephyra, was condemned by the gods as a punishment for his self-aggrandizing craftiness, to roll for eternity an immense boulder up a hill, only for it to roll down when it neared the top. Reflecting about the GDPR in light of this beautiful myth, we are faced with the following question: Is regulating health data privacy a similar Sisyphean task, doomed to fail under the big data tsunami or indeed under the complexities and the futility of legal regulation itself? To answer this, we need to examine two issues. First, a consideration of the appropriateness of data protection legal methodologies in the face of technological developments, and the new forms of health surveillance that these impose, is required. Second, the ways in which the EU legislator chose to 'catch up' with health data privacy issues must also be explored.

There are several reasons why this investigation matters. First, it can provide valuable insights about regulatory approaches to health data privacy and new technologies. For instance, does it make sense to divide data in categories (personal / non-personal, normal data / sensitive-health data, content data / metadata) and protect according to what the legislator deems as more important, or is this a meaningless exercise in the age of big data? Second, the way the law is shaped may have tremendously practical consequences for the use of new technologies. Even seemingly mundane choices of the legislator, such as the household exemption that makes the GDPR inapplicable to 'personal or household' activities[16] including social networking, may have pervasive implications for children's health data shared on social media by their parents. While the GDPR adopts a clear stance in favour of protecting children's data privacy, it is unclear what its position is in this regard.[17] Finally, important lessons about the GDPR's omnipotent ambition to regulate everything from personal data processed manually to algorithmic decision making and Artificial Intelligence (AI) can be learnt.

This book engages with these questions from a variety of perspectives and disciplinary lenses. The GDPR is a complex and evolving body of law that aims to deal with several technological and societal health data privacy problems, while safeguarding 'public health' interests and addressing its internal gaps and uncertainties. This very idea connects the chapters in this book.

The contributions that follow engage to this open dialogue, by offering new theoretical considerations and a taxonomy of health and big data-related

problems as well as solutions, proposals and models. The book is divided into two sections that encounter some of the most pressing and important debates concerning health data privacy and its regulation in the EU.

Section One focuses on the GDPR's approach regarding a variety of health data problems.

Chapter 1 explores the GDPR's provisions relating to health by focusing on two main issues: i) the definitional uncertainties surrounding health data and ii) the legislative choices regarding the balance between the competing interests to data privacy on the one hand, and the interests of 'public health' on the other hand. The chapter finds that the GDPR contains a broad definition of data concerning health and recognises augmented protection to these as sensitive data. This illustrates that the EU legislator considers health data privacy as an important interest often at risk that merits additional protection. At the same time, the GDPR includes several exemptions and restrictions to health data privacy interests. The chapter concludes that while the GDPR's provisions balancing data privacy with public health interests appear flexible and context dependent, its binary definitional distinctions (sensitive (health) / non-sensitive (non-health) data is problematic and may result in rendering the GDPR's rules both overinclusive and underinclusive.

Chapter 2 analyses the GDPR's legal definitions of (joint) controller and processor and their differing interpretation by competent Data Protection Authorities and the Court of Justice of the European Union (CJEU) within the context of three health-related case studies. In particular, the chapter examines how responsibility for compliance with the GDPR is attributed among the actors involved in the case of i) clinical trials, ii) health data processing within the global platforms, and iii) wearables at the workplace. Yordanka Ivanova concludes that there is a need for greater legal certainty in defining the capacity of the data processing actors and calls for a change in the Court's approach in defining the scope of joint controllership from 'single phase' to 'value chain'.

Chapter 3 considers the protections available to children under the GDPR and in United Kingdom (UK) law in respect to the oversharing of personal health information by parents on social media ('sharenting'). According to Rosemary Jay, the GDPR applies some limited safeguards to the processing of personal data about children, particularly in the area of online activity. Nevertheless, the borders of these safeguards are unclear. In particular, those with parental responsibility can post, share or otherwise make public, personal information about children as long as the parent can assert that they are carrying out a 'purely personal or household activity'. The case of 'sharenting' that may result, with potential detrimental effects on children, demonstrates the uncertainties and complexities that surround the scope of the GDPR.

Chapter 4 investigates the rules and conditions under which health data can be brought together on a European-wide platform for the purpose of big data analytics. To understand how the GDPR regulates the processing of health data for research purposes, Jos Dumortier and Mahault Piéchaud Boura make a distinction between research as a primary purpose of processing and

research as a secondary purpose. The chapter concludes that the GDPR has not created a harmonised regulatory framework for researchers who wish to perform research based on health data to be collected in multiple European countries. The authors argue that the complexity and fragmentation of the regulatory landscape is not in the first place a consequence of the GDPR having failed to reach its ambitions. Rules and procedures to be respected by researchers planning to use health data for research purposes are not exclusively imposed by data protection law but they are more often related to data ownership. This means that in practice, researchers are requested to meet the conditions set by the health data owners – healthcare institutions and private or public health data repositories. To overcome the complexity of the regulatory framework with which researchers are confronted, initiatives such as the European Commission's creation of European-wide repositories of health images or digital pathology slides are to be welcomed. If successful, the authors consider that such initiatives can shift the burden of bringing health data from different countries together from the researcher to the repository owners.

Chapter 5 examines issues of security and confidentiality concerning eHealth and mHealth applications. A number of technological solutions have been developed over the years to prevent security breaches and make user data information as secure as possible. These techniques include, among others, data modification, cryptographic methods and protocols for data sharing and query auditing methods. The authors argue that as years go by, privacy will continue to gain prominence in eHealth and mHealth and more investment will be made in this respect.

Section Two adopts a more critical approach to examine the GDPR's regulatory solutions on different questions that touch on health personal data.

In Chapter 6, Bart van der Sloot explains that the current data privacy legal regime distinguishes between different types and categories of data. In general, the more personal, private and sensitive data are, the higher the level of protection provided. Among others, the legal regime differentiates between non-personal data and personal data, between metadata and content data and between non-sensitive and sensitive personal data. The chapter goes on to provide three reasons why these legal categories may become redundant in the age of big data. First, it suggests that categorising data only works when the status of the data is relatively stable, while in the current and future technological environment their nature will be highly volatile. Second, it suggests that categorising data only works when it is possible to determine with relative certainty into which category data fall, while this will be ever more difficult because the sensitivity of the data is less and less a quality of the data and more and more a result of the efforts invested by parties having access to the data. Third, it suggests that the underlying rationale for laying down different regimes of protection for different categories of data may become redundant, because metadata can be just as or even more revealing than content communication data, personal data may reveal more sensitive aspects of people's lives than sensitive personal data and aggregated data may be used in ways that have a bigger impact on people

than the use of identifying data. The chapter argues that the status of data is not the right starting point for future legal regulation and suggests that as long as the status of data is taken as starting point for regulation, a strong regime should govern the processing of non-personal, non-sensitive and aggregated data in order to protect the interests of citizens.

Chapter 7 challenges the assumption that data privacy frameworks in general and the GDPR in particular can provide an appropriate regulatory solution for big data. It argues that in order to be able to properly reflect on regulatory approaches that wrestle with big data challenges, closer attention should be paid to these particular challenges. Searching for appropriate regulatory solutions requires a focus on the problems that need to be addressed. The chapter makes three distinct contributions to the debate regarding regulatory approaches to big data: First, it develops a taxonomy of big data challenges that allows a comprehensive overview of the issues at stake. Second, it examines the capabilities and limitations of the GDPR to address the risks identified in the proposed taxonomy. Third, it offers some suggestions on the pathways that regulators should be considering when approaching big data and AI.

Chapter 8 engages with two specific problems regarding the role and significance of the UK National Health Service (NHS) Code of Conduct's principles-based approach as critical to the UK government's vision for modernising healthcare. First, it questions the implication that data protection law, unlike the Code of Conduct, is a monolithic centralised framework of rigid rules which constrain the ability of relevant parties to tailor regulations to the novel use of technologies and data-driven processes in discharging their responsibilities towards patients. Second, a close examination of the Code of Conduct suggests that the GDPR already provides a legal infrastructure aimed at promoting a bottom-up approach of spontaneous 'regulatory conversations' with a view to speeding up access to personal information and minimise obstacles to collection, pave the way towards harnessing insights from the use of big data analytical systems and provide assurances of data quality and trustworthiness. Joseph Savirimuthu argues that many of the principles in the Code of Conduct that are perceived as being responsive to the challenges clinicians face in dynamic settings originate in the law's reflexive and flexible framework that is polycentric and provides mechanisms for steering actors processing health data at multiple levels, with the aim of ensuring that collective understandings of norms and practices being developed and operationalised are consistent with the GDPR.

Overall, the book aims to provide readers with new perspectives on health data privacy problems and regulatory solutions from a variety of different backgrounds and disciplines. It is certainly a peculiar time to be reflecting about health data privacy in the COVID-19 era of imposed social isolation and quarantines. Data privacy scholarship needs to be agile and ready to react to the challenges that emerge and that will continue to appear ahead of this unprecedented health emergency. Public health interests should be seriously taken into consideration while ensuring that these extraordinary circumstances and

the measures they require do not become the new ordinary as far as our fundamental rights and freedoms are concerned.

Keeping these thoughts in mind, I hope that the following pages, with their broad coverage of a diverse range of health data protection problems and perspectives, will provide the reader with interesting and thought-provoking discussions.

Maria Tzanou
Keele, April 2020

Notes

1 EDPS, Opinion 7/2015 *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability*, 7.
2 Paul Lewis, David Conn and David Pegg, 'UK Government Using Confidential Patient Data in Coronavirus Response', *The Guardian*, 12 April 2020 <www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response>.
3 Jack Nicas and Daisuke Wakabayashi, 'Apple and Google Team Up to "Contact Trace" the Coronavirus', *The New York Times*, 10 April 2020 <www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html>.
4 Andrew Roth et al., 'Growth in Surveillance May be Hard to Scale Back after Pandemic, Experts Say', *The Guardian*, 14 April 2020 <www.theguardian.com/world/2020/apr/14/growth-in-surveillance-may-be-hard-to-scale-back-after-coronavirus-pandemic-experts-say >.
5 Anita Allen, 'Protecting One's Own Privacy in a Big Data Economy' (2016) 130 *Harv. L. Rev. F.*, 71, 78.
6 Janet Burns, 'The "Spying Vibrator" Suit Is Over, But Sex Toys Are Still Talking Data', *Forbes*, 14 December 2016 <www.forbes.com/sites/janetwburns/2016/12/14/the-spying-vibrator-suit-is-over-but-sex-toys-are-still-talking-data/#692879384417>.
7 Janet Burns, 'We-Vibe Settles For $3.7M In "Spying Vibrator" Data Suit', *Forbes*, 15 March 2017 <www.forbes.com/sites/janetwburns/2017/03/15/we-vibe-settles-for-3-7m-in-spying-vibrator-data-lawsuit/#3ee371316021>.
8 Jessica Glenza, 'Revealed: Women's Fertility App is Funded by Anti-Abortion Campaigners', *The Guardian*, 30 May 2019 <www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners>.
9 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian*, 17 March 2018 <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
10 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), Official Journal of the European Union, L 119/1, 4 May 2016.
11 European Commission – Statement, Vice-President Ansip and Commissioner Jourová: Concluding the EU Data Protection Reform is Essential for the Digital Single Market, Brussels, 28 January 2015 <https://europa.eu/rapid/press-release_STATEMENT-15-3801_en.htm>.
12 Ibid.
13 European Commission, Communication from the Commission to the European Parliament and the Council, Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock, Brussels, 24.7.2019, COM(2019) 374 final, 2.

14 Ibid, 2. According to the Commission, '[o]ne key objective of the Regulation was to do away with a fragmented landscape of 28 different national laws that existed under the previous Data Protection Directive and to provide legal certainty for individuals and businesses throughout the EU. That objective has been largely met.'
15 EDPS Opinion 4/2015 *Towards a New Digital Ethics: Data, Dignity and Technology*, 11 September 2015, 12.
16 Article 2 (2) (c) GDPR. See also Recital 18.
17 See Chapter 3 in this book.

Acknowledgements

I would like to acknowledge the help of all the people involved in this project and, more specifically, to the authors and reviewers who took part in the review process.

This edited book has its origins in a workshop titled *Big Health Data and Social Media: Legal and Ethical Challenges*, which took place at Keele University School of Law in December 2017. I am deeply grateful to the Society of Legal Scholars (SLS) for funding this workshop. Without this generous support, this book would not have become a reality.

Finally, special thanks go to my family for their patience and understanding while completing this project.

Maria Tzanou
Keele University, UK

Section 1

Health data privacy under the GDPR

1 The GDPR and (big) health data

Assessing the EU legislator's choices

Maria Tzanou

1. Introduction

The COVID-19 pandemic has not only created an unprecedented health emergency in modern times across the globe; it has also brought forward a variety of data privacy issues. Imposed lockdowns, quarantines and 'self-isolation' measures are examples of what Anita Allen has coined as 'unpopular privacy'.[1] 'Unpopular privacy' refers to coercive mandates that 'impose unpopular privacies on intended targets and beneficiaries' like the COVID-19-related social distancing rules.[2] Schools and workplaces are closed; public events are cancelled; the use of public transport is limited;[3] people are even forbidden to do normal everyday activities,[4] such as sunbathing.[5] At the same time and in order to combat this pandemic, whole populations are required to endure increased surveillance of their location, their movements and their contacts[6] via the invasive monitoring of mobile phone data.[7]

Widespread health data surveillance is not a new phenomenon. Health data and the capture of their enormous potential through big data analytics have been at the forefront of recent debates, before the emergence of a global health pandemic. Data privacy regulatory responses to health data surveillance vary around the world, but the EU's General Data Protection Regulation (GDPR),[8] with its strengthened data privacy rules and principles, remains a point of reference. This chapter critically examines the GDPR's provisions relating to health by focusing on two main issues: i) the definitional uncertainties surrounding health data and ii) the legislative choices regarding the balance between the competing interests to data privacy on the one hand – seen mainly within the context of the enhanced protection that personal health data enjoy – and the interests of 'public health' on the other hand.

The analysis proceeds as follows: The following section assesses the definitional uncertainties that big health data raise. It takes a closer look at big data analytics and the sources of big health data and examines definitional questions within the GDPR's context. Section 3 discusses the GDPR's legislative choices regarding health data by focusing on their enhanced protection as 'special categories of data' and the exemptions and restrictions imposed on these for public health purposes. Section 4 offers brief conclusions.

2. On definitional issues: what are big health data?

2.1 Big data analytics

We are living in a big data world. Every minute, 510,000 comments are posted on Facebook, 293,000 statuses are updated, and 136,000 photos are uploaded. Every day, 3.5 billion Google searches are made; 6,000 tweets are sent per second; and more than 95 million photos and videos are uploaded on Instagram per day. There are 3.3 billion smartphone users worldwide, and the average smartphone user has between 60 and 90 apps on their device[9] collecting some kind of personal data (i.e., name, email address, location).[10] Outside the online world, the Internet of Things (IoT) 'merges physical and virtual worlds'[11] through a range of interconnected devices[12] that communicate data, such as smart thermostats, meters, doorbells, smoke alarms, cameras, digital assistants, TVs and refrigerators.[13] According to the European Commission, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually.

There is no commonly agreed-upon definition of 'big data'.[14] In broad terms, big data refers to the aggregation of huge volumes of diversely sourced information and their analysis, using sophisticated algorithms to inform decisions.[15] Big data is made possible due to the increasing capabilities of technology to support the collection and storage of large amounts of data, as well as 'its ability to analyse, understand and take advantage of the full value of data (in particular using analytics applications)'.[16] Big data is often described using the five Vs: Volume, Variety, Velocity, Veracity and Value.[17] Volume refers to the expanding amounts of data generated and the large-scale datasets; Variety relates to the different types of data and data sources; Velocity describes both the increasing speed at which data is produced and the increasing demand to analyse the data in near real time to get insights; Veracity[18] refers to the correctness and accuracy of the data; and Value denotes the opportunities of big data to lead to measurable improvements of our lives.[19]

Perhaps the most important characteristic of big data refers to the ways this is analysed. The full potential of big data can be realised using artificial intelligence (AI).[20] AI is needed to 'mine, parse, sort and configure the data into useful packages',[21] build models and draw inferences that are then used 'to predict and anticipate possible future events'.[22] This is often done through machine learning, namely 'algorithms that change in response to their own output, or "computer programs that automatically improve with experience"'.[23] Machine learning means that the system is able to train itself to learn continuously and modify its behaviour during operation, thus acquiring a level of autonomy.[24] Big data, AI and machine learning are closely related concepts and sometimes are referred to interchangeably. However, there are differences between the two. As the UK Government Office for Science astutely puts it: 'If data is the fuel, artificial intelligence is the engine of the digital revolution'.[25] As it might be more accurate in terms of terminology to use the umbrella concept 'big data

analytics' to describe all three of them.[26] That being said, this chapter and this book understand 'big data' as 'big data analytics' and the two terms are used interchangeably.

2.2 Big health data

Health data are at the centre of the big data revolution. Over 250,000 health and fitness apps are currently available on the market. The sale of wearables, such as smart watches, fitness trackers, eye gears, smart clothing, smart jewellery and implantables is on the rise, with more than 170 million wearables being purchased in 2018.[27] There are 'vagina fitbits',[28] smart vibrators, smart diapers,[29] and smart baby socks that measure babies' 'temperature, heart rate, oxygen saturation and movement'[30] available on the market. Our bodies emit streams of data: everything from physical activity, calorie intake, sleep and posture to sexual intercourse, menstrual cycles, fertility and breathing patterns can be (self)-tracked, measured, logged and (self)-analysed in order to achieve 'self-knowledge through numbers'.[31] The observation of our bodies through technologies is ingrained in our everyday lives, and global trends such as the Quantified-Self are constantly growing.[32] Platforms like PatientsLikeMe enable the exchange of information about illnesses, creating 'a community of people who are helping each other live their best every day'.[33] According to PatientsLikeMe, over '650,000 people living with 2,900 conditions have generated more than 43 million data points, creating an unprecedented source of real-world evidence and opportunities for continuous learning.'[34]

Big health data analytics promise a number of benefits. Indeed, the convergence between technology and healthcare is expected to i) increase quality of life and contribute to disease prevention,[35] and therefore reduce healthcare expenditure;[36] ii) allow 'better healthcare at a lower cost'; iii) foster 'patient empowerment (i.e. improved control over own healthcare)'; iv) enable 'easier and more immediate access to medical care and information online';[37] and v) develop 'more efficient and sustainable healthcare'.[38] Algorithmic analysis of huge datasets will develop 'personalised medicine' based on more accurate diagnostic predictions and treatment suggestions.[39] Such improvements are not an issue of the future; they are happening right now. Deep learning AI is already 'on a par with human experts'[40] when it comes to making medical diagnoses of diseases from cancers to eye conditions[41] based on images, and it might soon outperform humans. Big data analysis allows the discovery of previously unknown trends, correlations and patterns and, therefore, offers new valuable insights for medical research.[42]

2.3 On definitional uncertainties: what are 'big health data'?

Big health data are generated en masse and offer significant promises to improve our well-being and healthcare. If, therefore, we are to study carefully the challenges that the immense datafication of our bodies is posing and the ways the

law can approach these challenges, we need first to define what 'health data' and 'big health data' means.

Unlike its predecessor (the Data Protection Directive[43]), the GDPR contains a definition of 'data concerning health'. This can serve as a starting point for the present analysis. According to the GDPR, 'data concerning health' refers to 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.[44] Recital 35 further explains that

> personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU.[45] . . . to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

'Genetic data' as defined in the GDPR is also relevant to health data. The GDPR defines 'genetic data' as

> personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the *health* of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.[46]

The definition of 'health data' is not without problems. First, it appears tautological; it is not clear what is personal data related to the 'physical or mental health' or data that reveals information about a person's 'health status'. The GDPR does not define what constitutes 'health', although the term appears several times in this legislative instrument in different combinations: 'health status', 'public health', 'health purposes', 'health insurance', 'health security'. Nevertheless, it should be acknowledged that the definition of 'data concerning health' in the GDPR is quite broad. It includes healthcare data referring to medical history, diseases and disability, but also information about the past, current and future health status of the data subject, including disease risk.

The big data context complicates things even further. What about data generated outside the health care setting – for instance, fitness and well-being data captured through wearables and fitness apps? Are these considered 'health data'?

Completely trivial and innocuous data, such as supermarket shopping lists, may also reveal information about a person's dietary habits and, consequently, their health status. Indeed, it has been argued that a supermarket shopping database can be used to determine a 'person's current and future health status with a degree of accuracy comparable to that of a medical examination' with the ability to 'detect individuals' propensity to develop diseases such as diabetes, women's cancers, smoking-related cancers, cardiovascular disease, depression, etc.'[47] Furthermore, what constitutes health information can be context dependent; a piece of information might not possess the 'intrinsic nature'[48] of health data but, analysed by algorithms, it might reveal the health status of a person. The case, often cited by privacy scholars, of the department store Target sending a teenage girl ads about pregnancy products – before her family knew of her pregnancy – on the basis of her purchasing certain goods such as lotions and vitamin supplements,[49] demonstrates the potential of big data analytics. Definitional difficulties are exacerbated in the big data environment because data are not static, but dynamic; at one time point, they might be irrelevant to health or even not personal data at all (for instance, the levels of environmental pollution, weather data[50]), and at the next moment, combined and analysed with other datasets (i.e., lifestyle habits), they might reveal sensitive information.

It is not only that the meaning of 'health data' is blurred. Uncertainties also arise as to what constitutes 'big (health) data'. First, the term 'big' can be misleading in different ways.[51] The data is not always 'big'; it's their aggregation and analysis that matters. As Zuboff observes,

> 'big data' are constituted by capturing small data from individuals' computer-mediated actions and utterances in their pursuit of effective life. Nothing is too trivial or ephemeral for this harvesting: Facebook 'likes', Google searches, emails, texts, photos, songs, and videos, location, communication patterns, networks, purchases, movements, every click, misspelled word, page view, and more. Such data are acquired, datafied, abstracted, aggregated, analysed, packaged, sold, further analysed and sold again.[52]

It's not only that 'big data' is made by bits of 'small data'. It is also 'not always easy (or indeed useful) to say whether a particular instance of processing is or is not big data analytics.'[53] As technologies and algorithmic tools are increasingly ingrained in our lives, big data analytics are becoming the new normal, a part 'of business as usual'.[54]

Overall, the definitional boundaries of 'big health data' are not clear cut. What is 'big' data / what is 'small' data; what is 'health' data / what is not health data; what is personal data / what is non-personal data; what is 'big data analytics' and what is business as usual may differ from time to time and from context to context. The implications of these definitional uncertainties matter for this book. The GDPR considers 'data concerning health' as special categories of data (normally referred to as sensitive data) that merit enhanced protection.[55] Yet, the definitional difficulties discussed here cannot be resolved by merely

construing 'health data' broadly as proposed by the European Data Protection Supervisor (EDPS).[56] They demand a shift in thinking that can approach the problem in a novel, dynamic way that addresses the big data context.

That being said, this book adopts in general the not so accurate terminology of 'big health data' or 'big health data analytics' as an umbrella concept that covers broadly data generated from a variety of different sources and from which information about a person's health can be inferred. Some chapters focus on what can be seen as 'small' data instances of processing (such as sharenting), not losing sight of the fact that any information, however small, can be potentially rendered big data.[57]

2.4 Sources of big health data

Big health data can be captured in a variety of ways: i) it can be volunteered or surrendered by individuals when they share information about themselves (e.g., patient data shared with healthcare professionals) or third parties (e.g., their children); ii) monitored by tracking their activities (e.g., Google searches, loyalty schemes in gyms that record attendance, supermarkets that record purchasing history); and, finally, it can be 'inferred', based on the analysis or the 'profiling'[58] of volunteered, monitored and other data (e.g., health insurance premiums).[59] According to a report from the Organisation for Economic Co-operation and Development (OECD), the big data 'lifecycle' often follows the following sequence of steps: i) collection/access; ii) storage and aggregation; iii) analysis and distribution; and iv) usage.[60] Each step could potentially involve different stakeholders[61] and data could have several lifecycles entailing further aggregation and analysis.

There is a plethora of sources through which health information can be captured. Outside the traditional medical/healthcare sector, *mHealth* is an important source of big health data. Mobile Health ('mHealth') broadly refers to mobile devices and applications ('apps') that deliver health, well-being and lifestyle services and information.[62] These include wearables – data collection devices worn on the body, such as fitness trackers and smart watches – and health and fitness apps. mHealth solutions can be used to deliver a wide range of services,[63] including measuring and quantifying basic bodily functions (such as breathing rate, sleep, heart rate, blood pressure and blood glucose level) and habits (exercise patterns); offering medication reminders, fitness recommendations and nutritional advice; booking medical appointments; and assisting users with health-related questions. mHealth apps and devices routinely share users' data with third parties[64] such as advertisers. Apps can also be integrated with social media platforms in order to enhance users' experience by showcasing personal statistics and performances. Furthermore, wearables and apps can be used to facilitate 'gamification', understood as the 'use of game-like incentives'[65] (targets, competition) to encourage users to change their behaviour concerning physical activities[66] (i.e., walking) and even intimate relationships.[67]

mHealth devices and apps illustrate the potential of 'surveillance capitalism'.[68] As Lupton has noted,

> These devices could . . . be regarded as disciplinary, working to tame the . . . body by rendering it amenable to monitoring, tracking, and detailed analysis of the data thus generated. . . . These technologies configure a certain type of approach to understanding and experiencing one's body, an algorithmic subjectivity, in which the body and its health states, functions and activities are portrayed and understood predominantly via quantified calculations, predictions and comparisons.[69]

mHealth technologies are often connected to social media – for instance, a Fitbit can share the user's data on Facebook in order to showcase their performance. Social media platforms themselves contain important troves of health-related information. Facebook, Twitter, Instagram and PatientsLikeMe provide significant opportunities to form online communities – among others – around health issues, but they have also increased opportunities for health data surveillance.[70] For instance, PatientsLikeMe state that they share personal data, including information 'you provide about yourself to share with others like the condition you're living with and treatments you're trying' with the PatientsLikeMe community, as well as with partners that include universities, pharmaceutical companies, hospital systems, insurance companies, regulatory bodies and 'members of the Digital Life Alliance – like-minded digital health, science, and technology companies who work closely with PatientsLikeMe to improve health and healthcare around the globe'.[71]

3. On legislative choices: GDPR and health

3.1 The GDPR: an overview

The GDPR constitutes the centrepiece of EU data privacy law. It is a long and complex legislative document. It contains 173 (non-binding) Recitals and 99 provisions laying down 'rules relating to the protection of natural persons with regard to the processing[72] of personal data[73] and rules relating to the free movement of personal data'.[74] The GDPR does not apply to the processing of personal data that falls outside the scope of EU law; concerns national security policy; processing by a natural person in the course 'of a purely personal or household activity'; or processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[75]

In its substance, the GDPR is an omnibus regulation covering processing of personal data by both private and public bodies and addressing 'an immense landscape of potential informational problems'.[76] The provisions of the GDPR are structured around two main actors: the 'data subjects' and the 'controllers'. Data subjects are the natural persons whose personal data are processed. Controllers are the natural or legal persons, public authorities, or other bodies which, 'alone or jointly with others, determine the purposes and means of the

processing of personal data'.[77] National Data Protection Authorities (DPAs) oversee the application of the GDPR.[78]

The GDPR is a 'principles-based regulation'.[79] It includes six principles on the basis of which personal data must be processed: 'lawfulness, fairness and transparency'[80]; 'purpose limitation'[81]; 'data minimisation'[82]; 'accuracy'[83]; 'storage limitation'[84]; and 'integrity and confidentiality'.[85] An additional 'accountability' principle makes controllers responsible for complying with these data processing principles.[86]

Data subjects are granted a number of rights under the GDPR: a right of information,[87] access to,[88] rectification[89] and erasure[90] of personal data; a right to data portability;[91] a right to restrict[92] and object to certain types of processing;[93] and a right not to be subjected to fully automated decisions based on profiling.[94] Data breaches must be communicated by controllers to data subjects when they are likely to result in a high risk to the rights and freedoms of natural persons.[95]

The GDPR introduces a risk-based approach to data protection. Recital 75 explains that risks 'of varying likelihood and severity may result from personal data processing' and could lead to 'physical, material or non-material damage' and provides examples of such risk.[96] Controllers are obliged to undertake *ex ante* data protection impact assessments (DPIAs)[97] 'where a type of processing in particular using new technologies, . . . is likely to result in a high risk to the rights and freedoms of natural persons',[98] and notify *ex post* data breaches to supervisory authorities and the data subject[99] when they are 'likely to result in a high risk to the rights and freedoms of natural persons'.[100]

3.2 Health data under the GDPR

The GDPR contains a number of provisions on health data and health. Besides the definitional issues described previously, these concern on the one hand, the enhanced protection of health data as 'special categories of personal data',[101] and on the other hand, the exemptions and restrictions to data protection rules and principles for health reasons.

Health data enjoy increased levels of protection under the GDPR.[102] First, as a basic rule, the GDPR prohibits the processing of data concerning health.[103] There are several exceptions to this prohibition that will be discussed in the next section.

Second, the GDPR considers the processing of health data – and sensitive data in general – as one that might pose a 'risk' to the rights and freedoms of natural persons.[104] More fundamentally, there are cases where the GDPR views personal health data processing as 'high-risk'. For instance, the GDPR recognises that a high risk to the rights and freedoms of natural persons might arise when health data are processed 'on a large scale'[105] and obliges controllers to carry out a DPIA in this context.[106] This would include the case of a large hospital processing patients' genetic and health data,[107] although the GDPR is careful to point out that the processing of personal data of patients by an

individual physician or other health care professional would not be considered as 'large-scale'.[108]

Third, the GDPR prohibits automated decision-making including profiling,[109] which produces legal effects concerning a person or significantly affects her to be undertaken based on health data, unless the data subject has given her explicit consent or processing is necessary for reasons of substantial public interest and suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.[110] The GDPR grants data subjects the right not to be subject to fully automated decisions that analyse or predict aspects concerning their health[111] and obliges controllers to undertake a DPIA if they engage in such a systematic and extensive evaluation of natural persons based on automated processing, including profiling.[112]

Fourth, the GDPR specifically mentions the data subject's rights of information and access in relation to their health data. These include the right for data subjects to have 'access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided'.[113]

Fifth, additional responsibilities are imposed on controllers processing health data: these must keep records of processing activities even if the organisation employs fewer than 250 persons;[114] they must designate a Data Protection Officer (DPO) if the core activities of the controller or the processor consist of processing health data on a large scale;[115] and controllers and processors not established in the EU must designate in writing a representative in the Union if they process health data on a large scale.[116]

3.3 Exemptions allowing health data processing

The GDPR contains a number of exceptions to the (in principle) prohibition of processing of health data.[117] First, the processing of health data is allowed if the data subject has given her 'explicit consent'.[118] It should be recalled that the GDPR has significantly raised the substantive and procedural requirements on 'consent' for the processing of personal data in general;[119] the bar is even higher when special categories of data, and therefore, health data, are at issue. The GDPR even allows Member States or the EU under certain instances to remove the consent exception altogether.[120]

Health data can also be processed when this is necessary to protect the 'vital interests' of the data subject or of another person when they are physically or legally incapable of giving their consent[121] (e.g., the data subject is unconscious after an accident, and the hospital needs to know her medical history, whether she has any allergies or uses any medication). Health data processing is further allowed where this has been 'manifestly made public by the data subject'.[122] This provision creates a number of uncertainties because, as mentioned earlier, mHealth apps and devices (such as Fitbits) often share users' information on social media and individuals frequently post health-related information

on social media platforms both generic (Facebook, Twitter, etc.) and specific (PatientsLikeMe). The GDPR seems to permit the processing of health data in this respect,[123] but I submit that the mere posting of health data on social media would not be enough to allow the processing of such data by another controller.

The processing of health data is also allowed when necessary for reasons of 'substantial public interest'.[124] It should be noted that the GDPR does not require the processing merely in the 'public interest'; the public interest must be 'substantial'. What constitutes 'substantial public interest' is not defined in the GDPR. Moreover, the GDPR allows the processing of health data when necessary,

> for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.[125]

Finally, the GDPR provides that Member States can maintain or introduce further conditions, including limitations, with regard to the processing of health, genetic data and biometric data.[126] This might contribute to the further fragmentation of the health data landscape in the EU and increase uncertainties.

3.4 'Public health' exceptions and restrictions

The GDPR enshrines several exemptions and restrictions of data protection rules for public health purposes. The processing of sensitive data – including health data – is allowed for reasons of public interest in the area of 'public health'.

'Public health' refers to:

> all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.[127]

Article 35 of the EU Charter of Fundamental Rights (EUCFR) guarantees a 'right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices' and provides that 'a high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities'.

More particularly, the GDPR permits the processing of health data when this is necessary to protect against 'serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices'.[128] The public interest in the area of public health

does not have to be 'substantial',[129] and this provision provides a basis for the processing of health data without needing any other legal basis (such as the data subject's explicit consent).[130] The GDPR warns, however, that such processing of health data for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.[131] Recital 46 GDPR states that '[s]ome types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread'.[132] The current COVID-19 pandemic would be an example of such processing of personal health data that would be considered in the public interest in the area of public health and, therefore, permitted.[133]

The GDPR allows restrictions to data protection principles and data subjects' rights taken on the basis of 'public health' purposes.[134] Such restrictions can be imposed by EU or Member States' law by way of a 'legislative measure' that respects the essence of the fundamental rights and freedoms and is necessary and proportionate in a democratic society.[135] The GDPR also includes a 'public health' exemption to the right to erasure ('right to be forgotten') that obliges controllers to erase personal data concerning a data subject if requested to do so.[136] This means that if further retention of the personal data is necessary for public health reasons, the controller is not obliged to erase them even if the data subject has exercised her right to erasure. Furthermore, the GDPR provides a number of derogations from the general rule that personal data can be transferred to third countries outside the EU only when these provide an adequate level of protection[137] or appropriate safeguards, including binding corporate rules.[138] A case where such international transfer can take place without appropriate safeguards or an adequacy decision is when the transfer is 'necessary for important reasons of public interest'[139] that include 'public health, for example in the case of contact tracing for contagious diseases'.[140] Such derogation could be used, for instance, to allow for the transfer of EU originating personal data to countries that do not guarantee an adequate protection to combat the COVID-19 pandemic and trace the contacts' spread of this virus.

Finally, the GDPR makes clear that it applies to personal data processed for 'scientific research purposes', including technological development and demonstration, fundamental research, applied research and privately funded research.[141] According to the GDPR, 'scientific research purposes' also include studies conducted in the public interest in the area of public health.[142] If the result of scientific research in the health context gives reason for further measures in the interest of the data subject, the general rules of the GDPR are also applicable to those measures.[143]

3.5 Assessing the GDPR's health-related legislative choices

Overall, it is clear that the GDPR's provisions examined previously constitute a legislative attempt to *balance* two distinct forms of fundamental values and

interests: those of data privacy and those of public health. Whether the GDPR achieves a fair balance in this respect, is a question that remains to be answered. However, a number of points can be raised in this regard.

First, the GDPR takes a clear position on the question 'for the benefit of whom' the balancing between the fundamental interests of data privacy and public health should be taking place. As Recital 53 puts it,

> Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes *for the benefit of natural persons and society as a whole . . .*[144]

This is a significant choice made by the EU legislator that provides the benchmark for the balancing exercise; this must always be undertaken for the benefit of individuals and the society as a whole.

Second, the question of balancing between data privacy interests on the one hand, and public health interests on the other hand, is a context-dependent one. These interests are prioritised differently depending on the context within which they arise: In situations- where the monitoring of epidemics and their spread is required – much like the current COVID-19 pandemic – public health interests are prioritised over data privacy. Under normal processing circumstances, data privacy interests are prioritised and the GDPR recognises increased levels of protection of 'health data' compared to normal sensitive data. There are exemptions, restrictions and exceptions under normal processing circumstances as well – these prioritise, in particular cases, public health interests. In this respect, the GDPR has done a good job, as it adopts a degree of flexibility when considering the different interests at stake.

Third, where public health restrictions are required, these must be prescribed by law, be necessary in a democratic society, respect the principle of proportionality and be accompanied with appropriate (data protection) safeguards. Such safeguards are crucial and must be respected even in exceptional times, such as the ongoing COVID-19 pandemic.[145]

What makes the GDPR's legislative choices more problematic, however, is their *binary* nature. This brings me to the fourth point I would like to make. The GDPR follows a 'black/white approach'[146] regarding health data privacy. The data are either sensitive or not; if they are, then they enjoy increased protections. They are either personal or not, and if they are, the data protection rules apply; if not, they fall altogether outside the scope of the GDPR. Such distinctions and dichotomies based on a binary approach are difficult to maintain in the big data analytics environment. They often make little sense and entail a risk of both regulatory overinclusiveness and underinclusiveness. Strict and rigid rules based on binary choices might not be necessary at every instance;[147] conversely, the GDPR's rules and protections regarding health data might fall short in effectively protecting individual and societal interests in certain cases.

4. Conclusion

The COVID-19 pandemic has brought forward a plethora of challenges, both known and unknown, that data privacy faces.[148] Health surveillance, however, is hardly new. This has often taken place also outside the traditional healthcare context through a variety of mHealth apps, devices and social media platforms.

The GDPR contains a broad definition of data concerning health and recognises augmented protection to these as sensitive data. This illustrates that the EU legislator considers health data privacy as an important interest, often at risk, that merits additional protection. At the same time, the GDPR includes several exemptions and restrictions to health data privacy interests. Some of these are based on the individual circumstances of data subjects (e.g., 'explicit consent' or to protect the 'vital interests' of the data subject), but most of them concern public health interests.

The GDPR's provisions balancing data privacy with public health interests appear flexible and context dependent. In this regard, data protection rules 'can in no manner be an obstacle to saving lives'[149] and 'do not hinder measures taken in the fight against the coronavirus pandemic'.[150] At the same time, exceptional measures should be adopted only when it is necessary and must be proportionate and followed by data privacy safeguards. This demonstrates that the GDPR enshrines the rule of law principle. Exceptional circumstances measures cannot appear and operate in a democracy vacuum; they must be taken in accordance with the rule of law and the principle of proportionality as they operate in a democratic society. This also confirms that the GDPR does not allow the exploitation of exceptional circumstances introduced to combat COVID-19 'to usher in an era of biosurveillance' that will persist even after the pandemic has ended.[151]

While the GDPR can be applauded for striking a reasonably fair balance between data privacy and public health interests, the binary, black/white approach it adopts regarding sensitive (health) / non-sensitive (non-health) is problematic. Such distinctions are difficult to make in a big data context using AI analytics and entail the risk of rendering the GDPR's rules both overinclusive and underinclusive.

Notes

1 Anita L. Allen, *Unpopular Privacy: What Must We Hide?* (New York: Oxford University Press, 2011).
2 Ibid.
3 For an overview of COVID-19 restrictive measures across the world, see Oxford University's COVID-19 Government Response Tracker project. Hale Thomas et al., 'Oxford COVID-19 Government Response Tracker', Blavatnik School of Government, 2020. Data use policy: Creative Commons Attribution CC BY standard <www.bsg.ox.ac.uk/research/research-projects/oxford-covid-19-government-response-tracker>.
4 See also Rebecca Ratcliffe, 'Teargas, Beatings and Bleach: The Most Extreme Covid-19 Lockdown Controls around the World', *The Guardian*, 1 April 2020 <www.theguardian.com/global-development/2020/apr/01/extreme-coronavirus-lockdown-controls-raise-fears-for-worlds-poorest>.

5 Alison Hills, "'Can I Sunbathe in the Park?" Is Now a Deep Moral Question', *The Guardian*, 10 April 2020 <www.theguardian.com/commentisfree/2020/apr/10/sunbathing-park-deep-moral-questions-philosophers-coronavirus-individual>.
6 Jack Nicas and Daisuke Wakabayashi, 'Apple and Google Team Up to "Contact Trace" the Coronavirus', *The New York Times*, 10 April 2020 <www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html>.
7 Alex Hern, 'Experts Warn of Privacy Risk as US Uses GPS to Fight Coronavirus Spread', *The Guardian*, 2 April 2020 <www.theguardian.com/technology/2020/apr/02/experts-warn-of-privacy-risk-as-us-uses-gps-to-fight-coronavirus-spread>.
8 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), Official Journal of the European Union, L 119/1, 4 May 2016.
9 Gillian Cleary, 'Mobile Privacy: What Do Your Apps Know About You?', 16 August 2018 <www.symantec.com/blogs/threat-intelligence/mobile-privacy-apps>.
10 Art 29WP Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013.
11 European Commission, 'Digital Single Market Policy: The Internet of Things', <https://ec.europa.eu/digital-single-market/en/internet-of-things>.
12 The European Commission estimates that the number of IoT connections will raise to 6 billion by 2020. Commission Staff Working Document, Advancing the Internet of Things in Europe, Accompanying the document Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market {COM(2016) 180 final}, Brussels, 19.4.2016 SWD(2016) 110 final. See also, Art 29 WP, *Opinion 8/2014 on Recent Developments on the Internet of Things*, adopted on 16 September 2014; Samuel Greengard, *The Internet of Things* (Cambridge, MA: MIT Press, 2015).
13 Kari Paul, 'Teen Claims to Tweet from Her Smart Fridge – But Did She Really?', 13 August 2019 <www.theguardian.com/technology/2019/aug/13/teen-smart-fridge-twitter-grounded>.
14 On the meaning of 'data' and 'information' in the law in general and in data protection laws see Lee Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35 (1) *Oxford Journal of Legal Studies*, 91.
15 EDPS, Opinion 7/2015 *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability*, 7.
16 Ibid.
17 Kitchin argues that there are seven dimensions to big data, including exhaustivity, resolution and indexicality, relationality and extensionality and scalability. Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences* (London: Sage, 2014). Rob Kitchin and Gavin McArdle, 'What Makes Big Data, Big Data? Exploring the Ontological Characteristics of 26 Datasets' (2016) 3 (1) *Big Data and Society*, 1.
18 Variability is also often mentioned. This means that data captured may vary from time to time or place to place. Anil Jain, 'The 5 V's of Big Data', 17 September 2016 <www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/>.
19 Sander Klous, 'Sustainable Harvesting of the Big Data Potential', in Bart van der Sloot et al. (eds.), *Exploring the Boundaries of Big Data* (Amsterdam: Amsterdam University Press, 2016), 27, 28.
20 UK Government Office for Science, *Artificial Intelligence: Opportunities and Implications for the Future of Decision Making*, 9 November 2016, 5.
21 John Danaher et al., 'Algorithmic Governance: Developing a Research Agenda through the Power of Collective Intelligence' (2017) *Big Data & Society*, 1, 2.

22 UK Government Office for Science, n 20, 5.
23 Ibid, 6.
24 Ibid, 7.
25 Ibid, 4.
26 Information Commissioner's Office (ICO), *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, 20170904 Version: 2.2, para 11.
27 Sarah Perez, 'IDC: Apple Led Wearables Market in 2018, with 46.2M of the Total 172.2M Devices Shipped', 5 March 2019 <https://techcrunch.com/2019/03/05/idc-apple-led-wearables-market-in-2018-with-46-2m-of-the-total-172-2m-devices-shipped/>.
28 Oliver Wainwright, 'KGoal: Introducing the Fitness Tracker for your Vagina', *The Guardian*, 4 July 2014 <www.theguardian.com/artanddesign/architecture-design-blog/2014/jul/04/kgoal-fitness-tracker-vagina-pelvic-floor>.
29 Arwa Mahdawi, 'Is Buying a "Smart Nappy" Really Such a Clever Idea?', *The Guardian*, 24 July 2019 <www.theguardian.com/commentisfree/2019/jul/24/is-buying-a-smart-nappy-really-such-a-clever-idea?CMP=Share_AndroidApp_Gmail>.
30 Richard Godwin, '"You Can Track Everything": The Parents Who Digitise their Babies' Lives', *The Guardian*, 2 March 2019 <www.theguardian.com/lifeandstyle/2019/mar/02/apps-that-track-babies-and-give-data-to-tech-firms-parents>.
31 See Quantified Self, 'Self Knowledge Through Numbers' <https://quantifiedself.com/>.
32 Deborah Lupton, *The Quantified Self* (Cambridge: Polity Press, 2016).
33 See <www.patientslikeme.com/about>.
34 Ibid. 'Today, PatientsLikeMe is the world's largest personalized health network . . . Everything members have shared empowers the community with personal agency, establishing PatientsLikeMe as a clinically robust resource that has published more than 100 research studies.'
35 European Commission, Green Paper on mobile Health ("mHealth"), Brussels, 10.4.2014, COM(2014) 219 final, 4.
36 Deborah Lupton, 'Quantifying the Body: Monitoring and Measuring Health in the Age of mHealth Technologies' (2013) 23 (4) *Critical Public Health*, 393.
37 EDPS, Opinion 1/2015 *Mobile Health: Reconciling Technological Innovation with Data Protection*, 21 May 2015, 3.
38 Commission, Green Paper on mHealth, n 35, 5.
39 Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 *B.C.L. Rev.*, 93, 102 <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>.
40 Nicola Davis, 'AI Equal with Human Experts in Medical Diagnosis, Study Finds', *The Guardian*, 24 September 2019 <www.theguardian.com/technology/2019/sep/24/ai-equal-with-human-experts-in-medical-diagnosis-study-finds?CMP=Share_AndroidApp_Gmail>.
41 Ian Sample, '"It's Going to Create a Revolution": How AI is Transforming the NHS', *The Guardian*, 4 July 2018 <www.theguardian.com/technology/2018/jul/04/its-going-create-revolution-how-ai-transforming-nhs>.
42 EDPS, Opinion 1/2015 *Mobile Health*, n 37, 9.
43 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, OJ L 281, 23/11/1995, p. 31.
44 Article 4 (15) GDPR.
45 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45.
46 Article 4 (13) GDPR. Emphasis added.
47 Antoinette Rouvroy, '"Of Data and Men" Fundamental Rights and Freedoms in a World of Big Data', Bureau of the Consultative Committee of the Convention for the

Protection of Individuals with regard to Automatic Processing of Personal Data [ETS 108], p. 27.

48 EDPS, Opinion 1/2015 *Mobile Health*, n 37, 6.

49 Kashmir Hill, 'How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did', *Forbes*, 16 February 2012 <www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#d4fc43566686>.

50 Mr Dehaye, a Belgian national, received an email from The Weather Company, owned by IBM, that informed him that 'based on hot weather conditions in Mr Dehaye's area he was likely to have an "overactive bladder" – and buy more drinks' 9 June 2019. See Aliya Ram and Madhumita Murgia, 'Data Brokers: Regulators Try to Rein in the "Privacy Deathstars"', *Financial Times*, 8 January 2019 <www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521>.

51 See Matthew Jones, 'What We Talk About When We Talk About (Big) Data' (2019) 28 *Journal of Strategic Information Systems*, 3. Jones argues that '[r]ather than being a referential, natural, foundational, objective and equal representation of the world, . . ., data are partial and contingent and are brought into being through situated practices of conceptualization, recording and use.'

52 Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 *Journal of Information Technology*, 75, 79.

53 ICO, *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, n 26, 13.

54 Ibid.

55 See Art 9 GDPR.

56 EDPS, Opinion 1/2015 *Mobile Health*, n 37, 6.

57 Helen Nissenbaum has stated 'anything about an individual that can be rendered in digital form can be stored over indefinitely long periods and be readily retrieved.' See Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Wash. L. Rev.*, 119, 129.

58 Recital 71 GDPR explains that profiling 'consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.' For further details on the challenges posed by profiling, see Tzanou's chapter in this book.

59 OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value', OECD Digital Economy Papers, No. 220, OECD Publishing, 2013 <http://dx.doi.org/10.1787/5k486qtxldmq-en>, 10.

60 Ibid.

61 Ibid.

62 The Commission states that mHealth covers 'medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices. It also includes . . . lifestyle and wellbeing apps that may connect to medical devices or sensors (e.g. bracelets or watches) as well as personal guidance systems, health information and medication reminders provided by sms and telemedicine provided wirelessly.' See Commission, Green Paper on mHealth, n 35, 3.

63 For a theoritisation of the mHealth phenomenon, see Lupton, n 36.

64 For a very interesting empirical study, see Quinn Grundy et al., 'Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis' (2019) 364:1920 *BMJ*, 1.

65 John Danaher, Sven Nyholm and Brian D. Earp, 'The Quantified Relationship' (2018) *The American Journal of Bioethics*, 3.

66 Ali Shameli et al., 'How Gamification Affects Physical Activity: Large-Scale Analysis of Walking Challenges in a Mobile Application' (2017) *Proc Int World Wide Web Conf.*,

455; Rekesh Corepal et al., 'Exploring the Use of a Gamified Intervention for Encouraging Physical Activity in Adolescents: A Qualitative Longitudinal Study in Northern Ireland' (2018) *BMJ Open*, 0:e019663.

67 Danaher et al., n 21.

68 Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 *Journal of Information Technology*, 75. See also Tereza Hendl, Bianca Jansky, and Verina Wild, 'From Design to Data Handling. Why mHealth Needs a Feminist Perspective', in Loh, J. and Coeckelbergh, M. (eds.), *Feminist Philosophy of Technology* (Techno:Phil – Aktuelle Herausforderungen der Technikphilosophie, vol. 2) (Stuttgart: J.B. Metzler, 2019), 77.

69 Deborah Lupton, 'Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps' (2014) 17 *Culture, Health & Sexuality*, 440.

70 Frank Pasquale and Tara Adams Ragone, 'Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing' (2014) 17 *Stan. Tech. L. Rev.*, 595, 632.

71 PatientsLikeMe, 'Privacy Policy' <www.patientslikeme.com/about/privacy>.

72 According to Article 4 (2), 'processing' means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

73 According to Article 4 (1), 'personal data' means 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

74 Art 1 (1) GDPR.

75 Art 2 (2) GDPR.

76 Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What it is and What it Means' (2019) 28 (1) *Information & Communications Technology Law*, 65, 67.

77 Art 4 (7) GDPR.

78 See Article 51 GDPR.

79 Hoofnagle, van der Sloot and Borgesius, n 76, 67.

80 Article 5 (1) (a): Personal data should be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'.

81 Article 5 (1) (b): Personal data should be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes'.

82 Article 5 (1) (c): Personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

83 Article 5 (1) (d): Personal data should be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

84 Article 5 (1) (e): Personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.

85 Article 5 (1) (f): Personal data should be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

86 Article 5 (2) GDPR.

87 Articles 13 and 14 GDPR.
88 Article 15 GDPR.
89 Article 16 GDPR.
90 Article 17 GDPR. Article 17 is entitled 'Right to erasure ("right to be forgotten").
91 Article 20 GDPR.
92 Article 18 GDPR.
93 Article 21 GDPR.
94 Article 22 GDPR.
95 Article 34 (1) GDPR.
96 The processing may give rise to 'discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; . . . data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; . . . personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; . . . personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; . . . personal data of vulnerable natural persons, in particular of children, are processed; or . . . processing involves a large amount of personal data and affects a large number of data subjects'.
97 Articles 35, 36 GDPR and Recital 76. For an ethical and social impact assessment see Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 *Computer Law & Security Review*, 754.
98 Article 35 (1) GDPR.
99 Articles 33 and 34 GDPR.
100 Article 34 (1) GDPR.
101 Article 9 GDPR.
102 According to Recital 53 '[s]pecial categories of personal data . . . merit higher protection'.
103 Article 9 (1) GDPR.
104 Recital 75 GDPR.
105 Article 35 (3) (b) GDPR.
106 Ibid. See also Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, WP248, 4 April 2017.
107 Hoofnagle, van der Sloot and Borgesius, n 76, 87.
108 Recital 91 GDPR.
109 According to Article 4 (4) GDPR 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's . . . health . . . '
110 Article 22 (4) GDPR.
111 Recital 71 GDPR.
112 Article 35 (3) (a) GDPR.
113 Recital 63 GDPR.
114 Article 30 (5) GDPR.
115 Article 37 (1) (c) GDPR.
116 Article 27 (2) (a) GDPR.
117 Article 9 (2) GDPR. Only the ones most relevant to health data are discussed here.
118 Article 9 (2) (a) GDPR.
119 See Hoofnagle, van der Sloot, and Borgesius, n 76, 72.

120 Article 9 (2) (a) GDPR.
121 Article 9 (2) (c) GDPR.
122 Article 9 (2) (e) GDPR.
123 See Hoofnagle, van der Sloot and Borgesius, n 76, 83.
124 Article 9 (2) (g) GDPR. Such processing must be undertaken on the basis of Union or Member State law, must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
125 Article 9 (2) (h) GDPR. Such processing must be undertaken on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9 (3).
126 Article 9 (4) GDPR.
127 Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, OJ L 354, 31.12.2008, p. 70. See also Recital 54 GDPR.
128 Article 9 (2) (i) GDPR. Such processing must be undertaken on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
129 The European Data Protection Board (EDPD) seems to be requiring a 'substantial' public interest in this case too although this is not explicitly stated in Article 9 (2) (i) GDPR. See EDPD, Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, 2.
130 Article 9 (2) (i) GDPR requires that professional secrecy requirements, such as patient doctor confidentiality, should be respected in this case.
131 Recital 54.
132 See also Recitals 45, 52 and 54.
133 EDPD, n 129, 2.
134 Article 23 (1) (e) GDPR. See also Recital 73.
135 Ibid. According to Article 23 (2) GDPR such measures should 'contain specific provisions at least, where relevant, as to: (a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'
136 Article 17 (3) (c) GDPR. See also Recital 65.
137 Article 45 (3) GDPR.
138 Article 46 GDPR.
139 Article 49 (1) (d) GDPR. See also Article 49 (1) (f) that allows the transfer if it 'is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent'.
140 Recital 112 GDPR.
141 Recital 159 GDPR. See also Article 179 (1) TFEU.
142 Ibid.
143 [Endnote text is missing].
144 Emphasis added.
145 See EDPD, n 129, 1.
146 Nikolaus Forgo, 'My Health Data – Your Research: Some Preliminary Thoughts on Different Values in the General Data Protection Regulation' (2015) 5 (1) *International Data Privacy Law* 54, 59.
147 See, for example, Forgo who discusses medical research and argues that in certain cases this might produce (incidental) findings with relevance to the participants. 'In such

cases it might be necessary for the physician as an investigator to re-identify the trial participant'. Ibid, 58.

148 See, for instance revelations, that the UK government is sharing confidential National Health Service (NHS) patient data with private tech firms to build 'a COVID-19 datastore'. Paul Lewis, David Conn, and David Pegg, 'UK Government Using Confidential Patient Data in Coronavirus Response', *The Guardian*, 12 April 2020 <www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response>.

149 Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, Strasbourg, 30 March 2020.

150 EDPD, n 129.

151 This was argued by Edward Snowden. See David Pegg and Paul Lewis, 'NHS Coronavirus App: Memo Discussed Giving Ministers Power to "De-Anonymise" Users', *The Guardian*, 13 April 2020 <www.theguardian.com/world/2020/apr/13/nhs-coronavirus-app-memo-discussed-giving-ministers-power-to-de-anonymise-users>.

References

1 The chapter reflects the author's personal opinion as a researcher and is in no way engaging or presenting the position of the EU Institutions.
2 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.
3 Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169, 2010.
4 WP29, Opinion 1/2010, p. 2.
5 Article 5 GDPR.
6 Article 24 GDPR.
7 Article 35 GDPR.
8 Article 25 GDPR.
9 Recitals 18 and 91 GDPR.
10 Article 2 (2) (c) GDPR and Recital 18 GDPR.
11 WP29, Opinion 1/2010, pp. 9–10.
12 CJEU, C-131/12, *Google Spain*, ECLI:EU:C:2014:317, paras. 34 and 38; C-210/16, *Wirtschaftsakademie Schleswig-Holstein* (*Facebook fan page*), EU:C:2018:388, para. 28; C-40/17, *Fashion ID GmbH & Co. KG*, ECLI:EU:C:2019:629, para. 66.
13 CJEU, C-210/16, *Facebook fan page*, para. 68.
14 Ibidem, para. 38; Case C-25/17, *Yehovah's witnesses*, para. 69.
15 CJEU, C-25/17, *Yehovah's witnesses*, ECLI:EU:C:2018:551, para. 71.
16 CJEU, C-40/17, *Fashion ID GmbH & Co. KG*, ECLI:EU:C:2019:629.
17 Ibidem, paras. 78–79.
18 Ibidem, para. 80.
19 R. Mahieu, J. Hoboken, & H. Asghari, "Responsibility for Data Protection in a Networked World: On the Question of the Controller, 'Effective and Complete Protection' and Its Application to Data Access Rights in Europe", *JIPITEC*, Vol. 10 (2019), p. 86.
20 WP29, Opinion 1/2010, p. 16.
21 CJEU, C-40/17, *Fashion ID*, paras. 78–80.
22 Ibidem, paras. 74–75.
23 WP29, Opinion 1/2010, pp. 18–20.
24 Ibidem.
25 CJEU, C-210/16, *Facebook fan page*, paras. 28, 43, and 44; CJEU, C-25/17 *Yehovah's witnesses*, para.66; CJEU, C-40/17, *Fashion ID*, para. 70.
26 CJEU, C-25/17, *Yehovah's witnesses*, para. 71.
27 CJEU, C-210/16, *Facebook fan page*, para. 68.
28 CJEU, C-40/17, *Fashion ID*, para.80.
29 CJEU, C-25/17, *Yehovah's witnesses*, para.71.
30 CJEU, C-210/16, *Facebook fan page*, para.36.
31 CJEU, C-40/17, *Fashion ID*, paras.78–79.
32 Ibidem, para.76.
33 R. Mahieu & J. Hoboken, "Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?", *The Europeanlawblog*, 20 September 2019. Retrieved from <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/>.
34 Y. Ivanova, "Data Controller, Processor, or Joint Controller: Designing the Right Way for Reaching Compliance with the GDPR in a Data- and Technology-Driven World" (Forthcoming), in Tzanou, M. (ed.), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020).
35 WP29, Opinion 1/2010, p. 25.

36 Article 28 (2) and (4) of the GDPR.
37 Article 28 (10) GDPR. CJEU, C-101/01 *Bodil Lindqvist*, EU:C:2003:596, para. 47; CJEU, C-73/07 *Satakunnan Markkinapörssi and Satamedia*, EU:C:2008:727, para. 44; CJEU, C-212/13 *Ryneš*, EU:C:2014:2428, paras. 31 and 33, CJEU C-25/17 *Tietosuojavaltuutettu Jehovan todistajat (Yehovah's witnesses)*, ECLI:EU:C:2018, para. 40.
38 WP29, Opinion 1/2010, p. 25.
39 European Data Protection Supervisor, Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 2019.
40 WP29, Opinion 1/2010, pp. 24–30.
41 For example, according to the UK Information Commissioner's Office (ICO), accounting firms act always as independent controllers given that they have specific professional obligations, while the Bulgarian DPA has issued guidelines that accounting firms should instead be considered processors. Postal services are treated by WP29 as processors for the content of the messages and controllers when processing the personal data of the sender and recipient (e.g., names, contact details). By contrast, according to ICO, postal services do not have any capacity in relation to the content of the postal packages, as these are not considered to be data processing activities. By contrast, the Bulgarian DPA entirely treats postal services as independent controllers, given their obligations by law to ensure security and confidentiality of the delivery.
42 WP29, Opinion 1/2010, p. 32.
43 Ibidem.
44 Bulgarian Commission for Personal Data Protection, Opinion № НДМСПО-01–190/2019 Specifically on the Capacity of Data Controller or Processor in Clinical Trials and More Generally about the Distinction Guidelines on the GDPR, 2016. Retrieved from <www.cpdp.bg/index.php?p=element&aid=1163>.
45 Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance, OJ L 158, 27.5.2014, p. 1–76.
46 WP29, Opinion 1/2010, p. 30.
47 Article1 (2) c) of the GDPR.
48 CJEU, C-101/01, *Bodil Lindqvist*, EU:C:2003:596.
49 CJEU, C – 345/17, *Buivids*, ECLI:EU:C:2019:122.
50 CJEU, C- 131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2013:424, paras. 34–38.
51 Ibidem, para. 85.
52 CJEU, C-136/17, *GC and others v CNIL*, ECLI:EU:C:2019:773, paras. 45–47.
53 Ibidem, para.68.
54 Article 29 Working Party, Opinion 5/2009 on online social networking, WP 163, 2009.
55 P. Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge: Cambridge University Press, 2018), p. 157.
56 J. Baines, "ICO: Samaritans Radar Failed to Comply with Data Protection Act", 25 April 2015. Retrieved From <https://informationrightsandwrongs.com/2015/04/25/ico-samaritans-radar-failed-to-comply-with-data-protection-act/>.
57 Article 29 Working Party, Opinion 2/2017 on data processing at work, 17/EN WP 249, 2017, p. 18.
58 Kathryn Montgomery, Jeff Chester and Katharina Kopp, "Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment", *Journal of Information Policy*, Vol. 8 (2018), pp. 34–77.
59 Recital 43 of the GDPR states that 'consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the

circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance'.

60 Article 29 Working Party, Opinion 2/2017, p. 19.

61 Center of Data Ethics and Innovation, CDEI Snapshot Series, AI and Personal Insurance, September 2019.

62 See, for example, Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast)Text with EEA relevance, OJ L 26, 2.2.2016, pp. 19–59.

1 Children and the GDPR <www.ico.org.uk>.

2 Age Appropriate Design: A Code of Practice for Online Services. Draft code available at <www.ico.org.uk>.

3 April 2018.

4 See paper Stacey B. Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media' (2017) 66 *Emory L.J.* 839 for a US perspective.

5 For an analysis of the potential application of the law of confidence, tortious remedies, including Misuse of Private Information, see Claire Bessant, 'Sharenting: Balancing the Conflicting Rights of Parents and Children' (2018) 23 (1) *Communications Law*, 7–24, 1746–7616.

6 Schedule 6 DPA 2018. None of the amendments are relevant for the issues under consideration in this paper.

7 For example, OFCOM Communications Market report 2017 cited 42% of UK parents admitted to regularly sharenting.

8 The range of potential impacts is impressive, from embarrassment, shame and anxiety, concerns at the appropriation and misuse of images in pornography, concerns at children being targeted because their location is known, the use of information gleaned from posted material to groom children online and concerns about fraud and identity theft. There are also potentially positive outcomes, such as support for parents facing difficulties. See studies cited in Bessant (fn 4) and Steinberg (fn 3).

9 "Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration".

10 I am indebted to the White Paper produced by the Centre for Information Policy Leadership on Children and the GDPR for the material in this section.

11 6 November 2017 House of Lords Committee session.

12 20 September 2019.

13 Age Appropriate Design: A Code of Practice for Online Services – Consultation document April 2019 issued by the UK Information Commissioner <www.ico.org.uk>.

14 Ibid page 51.

15 Ibid page 54.

16 See FN 7.

17 GDPR Article 9.

18 Ibid Article 7.

19 Ibid Article 7 (3).

20 Ibid Article 15.

21 Ibid Article 21.

22 Ibid Article 17.

23 GDPR Article 2 (2)© DPA 2018 s.21(3).

24 DPA 2018 s.142(1)(b) (ii).

25 *Bodil Lindqvist v Kammar Aklagaren* (C-101/01) [2003] E.C.R.

26 See <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.
27 See fn 26.
28 Case C- 345/17 CJEU 14 February 2019.
29 [2011] EWHC 3185.
30 DPA 1998 s.36.
31 Case C-212-13.
32 [2017]EWCA Civ.
33 ICO, 'Social Networking and On-line Forums – When Does the DPA Apply?', 2014.
34 *Re D (A Child)*[2014] EWCA Civ 315, 'the concept of parental responsibility describes an adult's responsibility to secure the welfare of their child which is to be exercised for the benefit of the child not the adult. The all-encompassing nature of the responsibility underpins one of the principles of the Act which is the 'no order' principle in section 1(5) CA 1985: the expectation that all other things being equal parents will exercise their responsibility so as to contribute to the welfare of their child without the need for a court order defining or restricting that exercise.' per Ryder LJ.
35 DPA 2018 s.208.
36 Children and the GDPR <www. Ico.org.uk>.
37 Ibid page 41.
38 Final issued April 2018.
39 GDPR Article 4 (2).
40 See fn 36.
41 *Google Spain SL v AEPD C 131–12*.
1 Grant Agreement n°644906.; <www.aegle-uhealth.eu/en/>; In Greek mythology, "Aegle" is said to be one of the daughters of Asclepius and Epione. Her name has derived from "Αἴγλη" ("Aegle"), meaning "brightness," or "splendour," either from the beauty of the human body when in good health, or from the honour paid to the medical profession.
2 The platform is currently accessible at <www.biolytica.eu/>.
3 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).
4 <www.timelex.eu/en/horizon-projects/aegle>.
5 As stated in Recital 7 of the GDPR. See also Donnelly, M., & McDonagh, M. (2019). Health Research, Consent and the GDPR Exemption. *European Journal of Health Law*, 26(2), 97–119.
6 Molnár-Gábor, F. (2018). Germany: A Fair Balance Between Scientific Freedom and Data Subjects' Rights? *Human Genetics*, 137(8), 619–626.
7 Datatilsynet. (January 2018). Artificial Intelligence and Privacy, Report. *The Norwegian Data Protection Authority*, p. 17, available here: <www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.
8 Article 29's Working Party, Guidelines on Consent under Regulation 2016/679, WP 259, p. 27. See also Shabani, M., & Borry, P. (2018). Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation. *European Journal of Human Genetics*, 26(2), 149.
9 European Parliament, Panel for the Future of Science and Technology, European Parliamentary Research Service. (July 2019). How the General Data Protection Regulation Changes the Rules for Scientific Research. Report, available here: <www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf>.
10 European Parliament, Committee on Civil Liberties, Justice and Home Affairs. Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM(2012)0011-C7-0025/2012-2012/0011(COD)). Rapporteur: Jan Phillip Albrecht, p. 24,

available here: <www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN>.

11 M. Ploem, Essink-Bot, M. & Stronks, K. (2013). Proposed EU Data Protection Regulation is a Threat to Medical Research. *British Medical Journal*, 346, 3534; Dove, Edward S. *et al.* (September 6, 2014). Data Protection and Consent to Biomedical Research: A Step Forward? *The Lancet*, 384, 855.

12 Dove, E. & Laurie, G. (2015). Consent and Anonymisation: Beware Binary Constructions. *British Medical Journal*, 350, 1139.

13 EDPB, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR)[284] and the General Data Protection Regulation (GDPR), available here: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf>.

14 Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1). See also Recital 161 of the GDPR: *"For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council (1) should apply*".

15 See <www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>.

16 See also the European Court of Justice judgment of 1 October 2019 in Case C-673/17 (Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH).

17 Article 29 Working Party, Guidelines on consent under Regulation2016/679, WP 259 rev. 01, pp. 27–29.

18 Kaye, J., Whitley, E., Lund, D. *et al.* (2015). Dynamic Consent: A Patient Interface for Twenty-first Century Research Networks. *European Journal of Human Genetics*, 23, 141–146. See also Megan Prictor *et al.* (2019). Consent for Data Processing under the General Data Protection Regulation: Could 'Dynamic Consent' be a Useful Tool for Researchers? *Journal of Data Protection & Privacy*, 3(1), 93–112(20).

19 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, ELI: <http://data.europa.eu/eli/dir/2019/770/oj>.

20 Recital 12 of Directive (EU) 2019/770.

21 This opinion seems to shared by the European Data Protection Board in the Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 9 April 2019, p. 7: "*It is important to distinguish between entering into a contract and giving consent within the meaning of Article 6(1)(a), as these concepts are not the same and have different implications for data subjects' rights and expectations*".

22 Nederland Burgerlijk Wetboek (Dutch Civil Code), Book 7, Titel 7, Art. 458. For an English translation of the entire provision, see <www.dutchcivillaw.com/civilcode book077.htm>.

23 German federal data protection law, Section 22, § 2. An English translation, provided by the German federal Ministry of Interior, is available here: <https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf>.

24 Articles 4 (2) (k) and 6 of the Treaty on the Functioning of the European Union (TFEU), *OJ* C 326 of 26.10.2012, 47–390.

25 These three topics are: 1) organs and substances of human origin and blood and blood derivatives; 2) measures in the veterinary and phytosanitary fields; 3) medicinal products and devices for medical use. See article 168 TFEU.

26 See also van Veen, Evert-Ben. (November 2018). Observational Health Research in Europe: Understanding the General Data Protection Regulation and Underlying Debate. *European Journal of Cancer*, 104, 70–80, <https://doi.org/10.1016/j.ejca.2018.09.032>.

27 See Chapter IX of the French data protection law (Loi Informatique et Libertés); an English translation is available on the website of the CNIL: <www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>.
28 <www.registerforschung.at/ressourcen>.
29 The debate in Austria about the proposed access for research purposes to the electronic health record data has, according to the press media, resulted in over 5,000 patients opting out from the system. See <www.derstandard.at/story/2000079259475/5-000-elga-abmeldungen-wegen-forschungsdaten-debatte>.
30 See the Health Data Access Tool Kit, made available to researchers by the Medical Research Council, <https://hda-toolkit.org/story_html5.html>.
31 See Article 54 of the French law, available here: <www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>.
32 See, for example, the call for proposals DT-TDS-05–2020 under the Horizon 2020 programme (AI for health imaging), available here: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/dt-tds-05-2020>; also the call IMI2–2019–18–01 (Central repository of digital pathology slides to support the development of artificial intelligence tools), available here: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/imi2-2019-18-01>.

1 Vital Wave Consulting, 'MHealth for Development: The Opportunity of Mobile Technology for Healthcare in the Developing World' (Washington, DC and Berkshire, UK: UN Foundation-Vodafone Foundation Partnership, 2009).
2 Borja Martínez-Pérez, Isabel de la Torre-Díez and Miguel López-Coronado, 'Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis' (2013) 15 *Journal of Medical Internet Research* e120.
3 Basant Kumar, S.P. Singh and Anand Mohan, 'Emerging Mobile Communication Technologies for Health' (2010) *2010 International Conference on Computer and Communication Technology, ICCCT-2010*.
4 Mehdia Ajana El Khaddar and others, 'Emerging Wireless Technologies in E-Health: Trends, Challenges, and Framework Design Issues' (2012) *Proceedings of 2012 International Conference on Multimedia Computing and Systems, ICMCS 2012* 440.
5 Chin Feng Lin, 'Mobile Telemedicine: A Survey Study' (2012) 36 *Journal of Medical Systems* 511.
6 Sana Ullah and others, 'A Comprehensive Survey of Wireless Body Area Networks on PHY, MAC, and Network Layers Solutions' (2012) 36 *Journal of Medical Systems* 1065.
7 R. Gupta and M. Mitra, 'Wireless Electrocardiogram Transmission in ISM Band: An Approach Towards Telecardiology' (2014) 38 *Journal of Medical Systems* 90.
8 Neil Coleman, 'Mapping Subscribers for Better Mobile Networks' (2013) 12 *GEO: Connexion* 43.
9 Fabrizio Bert and others, 'Smartphones and Health Promotion: A Review of the Evidence' (2014) 38 *Journal of Medical Systems* 9995.
10 Farid Touati and Rohan Tabish, 'U-Healthcare System: State-of-the-Art Review and Challenges' (2013) 37 *Journal of Medical Systems* 9949.
11 Z. Xiao and F.E. Camino, 'The Fabrication of Carbon Nanotube Field-Effect Transistors with Semiconductors as the Source and Drain Contact Materials' (2009) 20 *Nanotechnology*.
12 Kenji Nakatani, 'New Technology Trends in Touch Panel Sensing' (2012) *Proceedings of the International Display Workshops*.
13 A. Benfdila and others, 'On the Drain Current Saturation in Carbon Nanotube Field Effect Transistors' (2010) 5 (3) *Nano* 161–165.
14 Matthias Bremer and others, 'The TV in Your Pocket: Development of Liquid-Crystal Materials for the New Millennium' (2013) 52 *Angewandte Chemie* 8880–8896.

15 Cynthia Kratzke and Carolyn Cox, 'Smartphone Technology and Apps Smartphone Technology and Apps: Rapidly Changing Health Promotion' (2012) 15 *International Electronic Journal of Health Education* 72–82.
16 J. Clement, 'Apple App Store: Quarterly Growth of Available Apps as 2015–2019' <www.statista.com/statistics/185722/apple-app-store-quarterly-growth-of-available-apps/> accessed 22 January 2020.
17 Research and Markets, 'MHealth Apps Market to Reach $236 Billion by 2026, Growing at a CAGR of 44.7% Over 2019–2026' (2019) <www.globenewswire.com/news-release/2019/08/21/1904780/0/en/mHealth-Apps-Market-to-Reach-236-Billion-by-2026-Growing-at-a-CAGR-of-44–7-Over-2019–2026.html> accessed 22 January 2020.
18 World Health Organization, 'MHealth: New Horizons for Health through Mobile Technologies' (2011) <www.who.int/goe/publications/goe_mhealth_web.pdf?ua=1> accessed 22 March 2020.
19 Hairong Yan and others, 'Wireless Sensor Network Based E-Health System – Implementation and Experimental Results' (2010) 56 (4) *IEEE Transactions on Consumer Electronics* 2288–2295.
20 Simon P. Cohn, 'Privacy and Confidentiality in the Nationwide Health Information Network', (*National Commitee on Vital and Health Statistics*, 2006).
21 Luke Irwin, 'The GDPR: What Exactly Is Personal Data?' <www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data> accessed 22 January 2020.
22 Ponemon Institute, '2017 Cost of Data Breach Study: Global Overview' (*IBM Security*, 2018), 47 <www.ibm.com/security/data-breach> accessed 4 April 2020.
23 Georg Disterer and Carsten Kleiner, 'BYOD Bring Your Own Device' (2013) 9 *Procedia Technology* 43.
24 The Wall Street Journal – Deloitte, 'Security and Privacy in Mobile Health' (2013) <http://deloitte.wsj.com/cio/2013/08/06/security-and-privacy-in-mobile-health/> accessed 22 March 2020.
25 Jennifer E. Moyer, 'Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage' (2013) 13 *Journal of Hospital Librarianship* 197 <www.tandfonline.com/doi/citedby/10.1080/15323269.2013.798768?scroll=top&needAccess=true>.
26 Disterer and Kleiner (n 23).
27 Elizabeth C. Whipple, Kacy L. Allgood and Elizabeth M. Larue, 'Third-Year Medical Students' Knowledge of Privacy and Security Issues Concerning Mobile Devices' (2012) 34 *Medical Teacher* e532.
28 Vodafone Global Enterprise, 'Evaluating MHealth Adoption Barriers: Privacy and Regulation – Protecting Your Patients Privacy in a Mobile World' (2013) <http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf> accessed 27 March 2020.
29 Chien Lung Hsu, Ming Ren Lee and Chien Hui Su, 'The Role of Privacy Protection in Healthcare Information Systems Adoption' (2013) 37 *Journal of Medical Systems* 9966.
30 Benjamin P. Rosenbaum, 'Radio Frequency Identification (RFID) in Health Care: Privacy and Security Concerns Limiting Adoption' (2014) 38 *Journal of Medical Systems* 19.
31 Hays Green, 'Strategies for Safeguarding Security of Mobile Computing' (2013) 67 *Healthcare Financial Management* 88.
32 Syeda Uzma Gardazi, Arshad Ali Shahid and Christine Salimbene, 'HIPAA and QMS Based Architectural Requirements to Cope with the OCR Audit Program' (2012) *Proceedings – 2012 3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, MUSIC 2012*.
33 David D. Luxton, Robert A. Kayl and Matthew C. Mishkind, 'MHealth Data Security: The Need for HIPAA-Compliant Standardization' (2012) 18 *Telemedicine and e-Health* 284.

34 Chang Kuo Yeh, Hung Ming Chen and Jung Wen Lo, 'An Authentication Protocol for Ubiquitous Health Monitoring Systems' (2013) 33 *Journal of Medical and Biological Engineering* 415.
35 Jiankang Ren, Guowei Wu and Lin Yao, 'A Sensitive Data Aggregation Scheme for Body Sensor Networks Based on Data Hiding' (2013) 17 *Personal and Ubiquitous Computing* 1317.
36 Xuelei Li and others, 'Secure Privacy-Preserving Biometric Authentication Scheme for Telecare Medicine Information Systems' (2014) 38 *Journal of Medical Systems* 139.
37 Chin Ling Chen and others, 'A Privacy Authentication Scheme Based on Cloud for Medical Environment' (2014) 38 *Journal of Medical Systems* 143.
38 Jung Tae Kim, 'Enhanced Secure Authentication for Mobile RFID Healthcare System in Wireless Sensor Networks' (2012) *Computer Applications for Database, Education, and Ubiquitous Computing*.
39 Ian Blair, 'Mobile App Download and Usage Statistics (2019)' (2019) <https://buildfire.com/app-statistics/> accessed 27 February 2020.
40 EU. GDPR, 'Article 35. "Data Protection Impact Assessment"' <www.privacy-regulation.eu/en/article-35-data-protection-impact-assessment-GDPR.htm> accessed 29 March 2020.
41 EU. GDPR, 'Article 9. "Processing of Special Categories of Personal Data"' <www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm> accessed 22 January 2020.
42 EU. GDPR, 'GDPR: Guidance on Consent Requirements' (2018) <www.cooley.com/news/insight/2018/2018-03-09-gdpr-guidance-on-consent-requirements> accessed 22 January 2020.
43 Public Law, 'Health Insurance Portability and Accountability Act of 1996. No. 104–191, 110 Stat.'
44 Barbara L. Filkins and others, 'Privacy and Security in the Era of Digital Health: What Should Translational Researchers Know and Do about It?' (2016) 8 *American Journal of Translational Research* 1560.
45 Federal Trade Commission, 'Act. 15 U.S.C.'
46 FTC Staff Report, 'Mobile Privacy Disclosures: Building Trust Through Transparency' (2013) <www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf> accessed 22 January 2020.
47 Public Law, 'Children's Online Privacy Protection Act of 1998 (COPPA). No. 105–277, 112 Stat.'
48 Timothy Phoenix Oblad and Elizabeth Trejos-Castillo, 'Children's Online Privacy Protection Act', in Marilyn Coleman and Lawrence Ganong (eds.), *The Social History of the American Family: An Encyclopedia* (Thousand Oaks, CA: SAGE Publications, Inc, 2014).
49 Stacey Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media' (2017) 66 *Emory Law Journal* 839 <https://ssrn.com/abstract=2711442>.
50 EU. GDPR, 'General Data Protection Regulation (GDPR)' (2016) <https://gdpr-info.eu/> accessed 22 January 2020.
51 Eirini Mougiakou and Maria Virvou, 'Based on GDPR Privacy in UML: Case of e-Learning Program' (2018) *2017 8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017*.
52 EU. GDPR, 'General Data Protection Regulation (GDPR)' (n 50).
53 A. Skendzic, B. Kovacic and E. Tijan, 'General Data Protection Regulation – Protection of Personal Data in an Organisation' (2018) *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 – Proceedings*.
54 Vodafone Global Enterprise (n 28).
55 Jin Wang and others, 'A Research on Security and Privacy Issues for Patient Related Data in Medical Organization System' (2013) 7 *International Journal of Security and its Applications* 287.

56 Sunil Kumar and Maninder Singh, 'Big Data Analytics for Healthcare Industry: Impact, Applications, and Tools' (2018) 2 *Big Data Mining and Analytics* 48.
57 Milica Milutinovic and Bart De Decker, 'Privacy-Preserving Data Management in EHealth Systems' (2013) 9 *Procedia Technology* 1085 <https://doi.org/10.1016/j.protcy.2013.12.121%0A>.
58 Bahar Farahani and others, 'Towards Fog-Driven IoT EHealth: Promises and Challenges of IoT in Medicine and Healthcare' (2018) 78 *Future Generation Computer Systems* 659 <https://doi.org/10.1016/j.future.2017.04.036>.
59 OWASP, 'OWASP Mobile Security Project' (2015) <www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks> accessed 22 January 2020.
60 Hadi Kharrazi and others, 'Mobile Personal Health Records: An Evaluation of Features and Functionality' (2012) 81 *International Journal of Medical Informatics* 579.
61 Vodafone Global Enterprise (n 28).
62 Michael McCarthy, 'Experts Warn on Data Security in Health and Fitness Apps' (2013) 347 *BMJ* (Clinical research ed.).
63 HealthCareBusinessTech, 'Mobile Health Apps Create Privacy Risk, Study Says' (2014) <www.healthcarebusinesstech.com/mobile-health-apps-privacy/> accessed 27 March 2020.
64 William Douglas Figg and Hwee Joo Kam, 'Medical Information Security' (2011) 5 *International Journal of Security (IJS)* 22.
65 ibid.
66 Pam Dixon, 'Medical Identity Theft – The Information Crime That Can Kill You' (2006) <www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/> accessed 9 February 2020.
67 M. Ahmed, M. Ahamad and T. Jaiswal, 'Augmenting Security and Accountability within the EHealth Exchange' (2014) *IBM Journal of Research and Development* <https://doi.org/10.1147/JRD.2013.2288068>.
68 B. Faudree and M. Ford, 'Security and Privacy in Mobile Health' (*CIO Journal*, 2013) <www.webcitation.org/6tp8fjE01> accessed 30 March 2020.
69 Qijun Gu and Mina Guirguis, *Secure Mobile Cloud Computing and Security Issues*, vol 9781461432 (2013).
70 John D. Piette and others, 'A Preliminary Study of a Cloud-Computing Model for Chronic Illness Self-Care Support in an Underdeveloped Country' (2011) 40 *American Journal of Preventive Medicine* 629.
71 Rui Zhang and Ling Liu, 'Security Models and Requirements for Healthcare Application Clouds' (2010) *Proceedings – 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*.
72 Joel J.P.C. Rodrigues and others, 'Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems' (2013) 15 *Journal of Medical Internet Research* e186.
73 Muzammil Hussain and others, 'A Security Framework for MHealth Apps on Android Platform' (2018) 75 *Computers and Security* 191.
74 Sahar Al-Dhahri, Manar Al-Sarti and Azrilah Abdul, 'Information Security Management System' (2017) 158 *International Journal of Computer Applications* 29.
75 OWASP (n 59).
1 International Bill of Human Rights: A Universal Declaration of Human Rights. <www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217(III)>.
2 International Covenant on Civil and Political Rights. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966. entry into force 23 March 1976, in accordance with Article 49. <www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.
3 Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950. <www.echr.coe.int/Documents/Convention_ENG.pdf>.
4 ECmHR, Campion v. France, application no. 25547/94, 06/09/1995. Unofficial Translation: In order to determine in similar cases the extent of the guarantee granted

by article 8 (art. 8) against interference by public authorities, the Commission examines whether the taking of photographs constitutes an intrusion into the private sphere of an individual (for example when these were taken at her home), if the photographs refer to private or public events, and if they are intended to be used for a limited purpose or they are likely to fall within the public's knowledge. In the present case, the Commission notes that the photograph for which the applicant complains was taken on the public highway, when he was traveling by car, for the purpose of proof and identification. Nothing indicates that the photograph has been brought to the attention of the public or used for any purpose other than the prosecution of which the applicant has been the subject. Applying the criteria set out earlier, the Commission comes to the conclusion that there has been no interference with the privacy of the applicant.

5 Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens (1973).

6 U. Dammann, O. Mallmann & S. Simitis (eds), *Data Protection Legislation: An International Documentation* (Engl) (Frankfurt am Main: Metzner, 1977). F. W. Hondius, *Emerging Data Protection in Europe* (Amsterdam: North-Holland, 1975). H. Burkert, *Freedom of Information and Data Protection* (Bonn: Gesellschaft für Mathematik und Datenverarbeitung, 1983).

7 Council of Europe Committee of Ministers Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Private Sector (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies). <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830>. Council of Europe Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Public Sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies). <https://rm.coe.int/16804d1c51>.

8 Charter of Fundamental Rights of the European Union (2000/C 364/01). <www.europarl.europa.eu/charter/pdf/text_en.pdf>.

9 Article 1 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. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>.

10 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). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

11 Article 2 sub a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981. <https://rm.coe.int/1680078b37>.

12 See for a discussion: B. van der Sloot, *Privacy as Virtue* (Cambridge: Intersentia, 2017).

13 Article 1 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>.

14 Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence Updated on 30 April 2019. <www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

15 ECtHR, Big Brother Watch and Others v. The United Kingdom, application nos. 58170/13, 62322/14 and 24960/15, 13 September 2018, § 356.

16 Article 9 GDPR.

17 Article 6 GDPR.

18 Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence Updated on 30 April 2019. <www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

19 Another source of inspiration could be the EU's e-Privacy Directive, which differentiates between traffic data, that are defined as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof, location data, meaning any data indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service, location data other than traffic data, etc. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
20 Joined cases C-203/15 and C-698/15 Tele2/Watson [2016] ECLI:EU:C:2016:970, para 99. For a full analysis of this CJEU judgment, see Will R. Mbioh, 'Post-och Telestyrelsen and Watson and the Investigatory Powers Act 2016' (2017) 3 (2) *EDPL* 273–282.
21 L. Taylor, L. Floridi & B. van der Sloot (eds), *Group Privacy* (Dordrecht: Springer, 2017), p. 284.
22 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2017. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. See also: Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP216, 10 April 2014. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.
23 P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review* 1701, p. 1723.
24 Ibid, p. 1704.
25 A. Fluitt et al., 'Data Protection's Composition Problem', (2019) 5 (3) *European Data Protection Law Review*.
26 Ibid.
27 See inter alia: Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:en:PDF>. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0037&from=FR>.
28 Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28 January 1981. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434>.
29 B. Greschbach, 'The Devil is in the Metadata – New Privacy Challenges in Decentralised Online Social Networks'. <www.nada.kth.se/~gkreitz/metadata/sesocMetaPrivacy.pdf>.
30 Article 1 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>.

1 For instance, Yeung notes: 'The right most clearly implicated by Big Data driven hypernudging is the right to informational privacy, given the continuous monitoring of individuals and the collection and algorithmic processing of personal digital data'. Karen Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design' (2017) 20 (1) *Information, Communication & Society*, 118, 124.
2 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), Official Journal of the European Union, L 119/1, 4 May 2016.
3 EDPS, Opinion 7/2015 *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability*.

4 Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) *Philosophical Transactions. R. Soc.* 1. The European Commission notes that 'the rules laid down in the [General Data Protection] Regulation provide a general framework and contain specific obligations and rights that are particularly relevant for the processing of personal data in AI'. See Commission, Communication from the Commission to the European Parliament and the Council, Data Protection Rules as a Trust-enabler in the EU and Beyond – Taking Stock, Brussels, 24.7.2019, COM(2019) 374 final.
5 For instance, the EDPS states: 'The question is not whether to apply data protection law to big data, but rather how to apply it innovatively in new environments.' EDPS, Opinion 7/2015, n 3, 4.
6 See Maria Eduarda Gonçalves, 'The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward' (2017) 26 (2) *Information & Communications Technology Law*, 90, 99.
7 Articles 35, 36 GDPR and Recital 76. For an ethical and social impact assessment see Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 *Computer Law & Security Review*, 754.
8 Article 35 (1) GDPR.
9 Articles 33 and 34 GDPR.
10 Article 34 (1) GDPR.
11 EDPS, Opinion 7/2015, n 3.
12 See Maria Tzanou, 'The GDPR and (Big) Health Data: Assessing the EU Legislator's Choices'.
13 Ibid.
14 Viktor Mayer-Schonberger and Yann Padova, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) *Colum. Sci. & Tech. L. Rev*, 315, 319.
15 See Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 *Seton Hall Law Review* 995, 1000.
16 See Ira Rubinstein and Woodrow Hartzog, 'Anonymization and Risk' (2016) 91 *Washington Law Review* 703, 710–711.
17 Article 4 (1) GDPR.
18 Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779. For case-note see Frederik Zuiderveen Borgesius, 'Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 (1) *European Data Protection Law Review*, 130.
19 Ibid, para 42.
20 Ibid, para 43.
21 Gloria González Fuster and Amandine Scherrer, 'Big Data and Smart Devices and their Impact on Privacy' (2015) *Study for the LIBE Committee*.
22 Ibid, 21. Schneier has developed a taxonomy of personal data, on the basis of social media that includes six categories: service data, which is provided to open an account (e.g., name, address, credit card information, etc.); disclosed data, which is entered voluntarily by the user; entrusted data, for example the comments made on other people's entries; incidental data, which refers to a specific user but is uploaded by someone else; behavioural data, which contains information about the actions users are undertaking when using the site and may be used for targeted advertising; and inferred data, which is information deduced from someone's disclosed data, profile or activities.
23 GDPR, Art. 7.
24 See Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.
25 Aleecia Mcdonald and Lorrie Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 (3) *I/S: A Journal of Law and Policy for the Information Society*, 543.

26 See José van Dijck, 'Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology' (2014) 12 (2) *Surveillance & Society*, 199; Nina Gerber, Paul Gerber and Melanie Volkamer, 'Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior' (2018) 77 *Computers and Security* 226.
27 See Tal Zarsky, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41 (1) *Science, Technology, & Human Values* 118.
28 Art. 7 (4) GDPR provides 'when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'
29 See Tzanou, 'Introduction', n 12.
30 See Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 189 and references therein.
31 GDPR, Article 6.
32 GDPR, Art. 5 (2).
33 Zarsky (n 15), 1020.
34 See Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Oxford: Hart Publishing, 2017), 26.
35 Ibid.
36 Zarsky (n 15), 1006.
37 Bart van der Sloot and Sascha van Schendel, 'Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study' (2016) *JIPITEC* 1, 10.
38 Ibid, 1006.
39 GDPR, Art. 5 (1) (c).
40 GDPR, Art. 5 (1) (e).
41 See Colin Bennett and Robin Bayley, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments', in Bart van der Sloot et al. (eds.), *Exploring the Boundaries of Big Data* (Amsterdam: Amsterdam University Press, 2016), 205, 210.
42 Ibid.
43 As put by the Dutch DPA in an empirical study 'Big Data is all about collecting as much information as possible.' See van der Sloot and van Schendel (n 37), 9.
44 Zarsky (n 15), 1011.
45 Ibid.
46 See van der Sloot and van Schendel (n 37), 9.
47 As eloquently put by van der Sloot and van Schendel 'Data can always be given a second life.' Ibid.
48 GDPR, Art. 5 (1) (d).
49 Ibid.
50 See relevant comments by Slovenian DPA as reported by van der Sloot and van Schendel (n 37), 9–10.
51 Ibid, 10.
52 Victor Mayer-Schoenberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work and Think* (London: John Murray, 2013), 15.
53 Van der Sloot and van Schendel (n 37), 9.
54 Article 5 (1) (b) GDPR.
55 Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis, Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123>, 2.
56 See Ernesto Damiani et al., 'Big Data Threat Landscape and Good Practice Guide', *ENISA*, January 2016. <www.enisa.europa.eu/publications/bigdata-threat-landscape> and Rossen Naydenov et al., 'Big Data Security. Good Practices and Recommendations

on the Security of Big Data Systems', *ENISA*, December 2015. <www.enisa.europa.eu/publications/big-data-security>.

57 See Antoinette Rouvroy, "'Of Data and Men" Fundamental Rights and Freedoms in a World of Big Data', Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS 108], 29.
58 Article 5 (1) (f) GDPR.
59 Article 32 GDPR.
60 Articles 33 and 34 GDPR.
61 Article 9 GDPR.
62 Article 9 (1) GDPR.
63 Article 9 (2) GDPR.
64 See Nathan Cortez, 'The Internet of Things (IoT) and Health Big Data: Introduction', in Glenn Cohen et al. (eds.), *Big Data, Health Law, and Bioethics* (Cambridge: Cambridge University Press, 2018), 125.
65 For details on health data sources see Introductory chapter. See also, Urs Grasser, 'Shifting Paradigms – Big Data's Impact on Health law and Bioethics: Introduction', in G. Cohen et al. (eds.), *Big Data, Health Law, and Bioethics* (Cambridge: Cambridge University Press, 2018), 15.
66 Moerel and Prins, n 55, 2.
67 Article 13 GDPR.
68 Article 15 GDPR.
69 Article 16 GDPR.
70 Article 17 GDPR. See also Maria Tzanou, 'The Unexpected Consequences of the EU Right to Be Forgotten: Internet Search Engines as Fundamental Rights Adjudicators', in M. Tzanou (ed.), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3277348>.
71 Article 18 GDPR.
72 See Article 21 GDPR.
73 Article 22 GDPR.
74 Rouvroy, n 57, p. 34.
75 Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) *Modern Law Review*, 428, 440.
76 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2016).
77 Ibid, 3.
78 See Tzanou, 'Introduction', n 12.
79 Mayer-Schoenberger and Cukier, n 52, 52.
80 González Fuster and Scherrer, n 21.
81 Mayer- Schoenberger and Cukier, n 52, 32.
82 'Garbage in, garbage out' refers to this problem. See Brent Daniel Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate' (2016) *Big Data & Society*, 1, 15.
83 Mayer-Schoenberger and Cukier, n 52, 66.
84 Mittelstadt et al., n 82, 6.
85 Pasquale, n 76, 3.
86 Mittelstadt et al., n 82, 6.
87 Jenna Burrell, 'How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data and Society*, 1.
88 Sharona Hoffman, 'Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease in Big Data', in Glenn Cohen et al. (eds.), *Big Data, Health Law, and Bioethics* (Cambridge: Cambridge University Press, 2018), 85, 85.
89 Ibid.
90 Mittelstadt et al., n 82, 6.

91 Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review*, 671.
92 Ibid.
93 Allison Gardner, 'Medical AI Can Now Predict Survival Rates – But It's Not Ready to Unleash on Patients', *The Conversation*, 21 November 2019 <https://theconversation.com/medical-ai-can-now-predict-survival-rates-but-its-not-ready-to-unleash-on-patients-127039> and references therein; Angela Lashbrook, 'AI-Driven Dermatology Could Leave Dark-Skinned Patients Behind', *The Atlantic*, 16 August 2018 <www.theatlantic.com/health/archive/2018/08/machine-learning-dermatology-skin-color/567619/>.
94 Ibid.
95 Zarsky, n 15, 1000.
96 Art 4 (4) GDPR defines profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.
97 Paul De Hert and Hans Lammerant, 'Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever?', in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds.), *Exploring the Boundaries of Big Data* (Amsterdam: Amsterdam University Press, 2016), 145, 147. The Art 29 WP identifies four stages of the profiling process: 1) collecting data; 2) analysing data; 3) building a profile for an individual; 4) applying a profile to make a decision affecting the individual. See Art 29WP, Guidelines on Automated individual decision-making and Profiling.
for the purposes of Regulation 2016/679, Adopted on 3 October 2017, 12.
98 Hildebrandt and Koops, n 75, 440.
99 De Hert and Lammerant, n 97, 147.
100 Ibid.
101 Ibid.
102 Ibid.
103 Article 29WP, Guidelines on Automated individual decision-making n 97, 5.
104 See previously described discrimination.
105 See previously discussed incorrect and unreliable conclusions.
106 See David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' (2014) *Big Data & Society* 1, 10.
107 European Data Protection Supervisor (EDPS), EDPS Opinion 4/2015 *Towards a New Digital Ethics: Data, Dignity and Technology*, 11 September 2015, 13.
108 Hildebrandt and Koops, n 75, 434.
109 See Maria Tzanou, 'European Union Regulation of Transatlantic Data Transfers and Online Surveillance' (2017) 17 (3) *Human Rights Law Review* 545–556.
110 Annex VI, Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU – US Privacy Shield, Brussels, 12 July 2016, COM (2016) 4176 final, 93.
111 See Tzanou, n 109.
112 Lyon, n 106.
113 Ibid.
114 Janet Burns, 'We-Vibe Settles For $3.7M In "Spying Vibrator" Data Suit', *Forbes*, 15 March 2017 <www.forbes.com/sites/janetwburns/2017/03/15/we-vibe-settles-for-3-7m-in-spying-vibrator-data-lawsuit/#3ee371316021>.
115 Janet Burns, 'The "Spying Vibrator" Suit Is Over, But Sex Toys Are Still Talking Data', *Forbes*, 14 December 2016 <www.forbes.com/sites/janetwburns/2016/12/14/the-spying-vibrator-suit-is-over-but-sex-toys-are-still-talking-data/#692879384417>.
116 Yeung, n 1, 123.
117 Lyon, n 106, 4.
118 Ibid.

119 For example, see Samuel Gibbs, 'Women Less Likely to be Shown Ads for High-Paid Jobs on Google, Study Shows', *The Guardian*, 8 July 2015 <www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>.
120 EDPS, Opinion 4/2015, n 107, 13.
121 Rob Kitchin, 'Thinking Critically about and Researching Algorithms' (2017) 20 (1) *Information, Communication & Society*, 14, 19.
122 EDPS, Opinion 4/2015, n 107, 13.
123 See OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value' (2013) OECD Digital Economy Papers, No. 220, OECD Publishing <http://dx.doi.org/10.1787/5k486qtxldmq-en>.
124 Ibid.
125 EDPS, Opinion 8/2016, Opinion on coherent enforcement of fundamental rights in the age of big data, 23 September 2016, 13.
126 Federal Trade Commission (FTC), *Data Brokers: A Call for Transparency and Accountability*, May 2014.
127 EDPS, Opinion 8/2016, n 125, 13.
128 Ibid.
129 Jessica Glenza, 'Revealed: Women's Fertility App is Funded by Anti-Abortion Campaigners', *The Guardian*, 30 May 2019 <www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners> and Eva Wiseman, 'Beware the Fertility App that Wants to Share Your Data with Anti-Abortion Campaigners', *The Guardian*, 9 June 2019 <www.theguardian.com/lifeandstyle/2019/jun/09/app-creep-and-the-dark-side-of-sharing-private-date-on-our-phones>.
130 Kitchin, n 121, 19.
131 Accountability is understood differently here from the 'accountability principle' under Article 5 (2) GDPR.
132 Pasquale, n 76, 217.
133 Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 *Journal of Information Technology*, 75, 83 and 85.
134 See earlier.
135 Gonçalves, n 6, 114.
136 Zarsky, n 15.
137 Art 29 WP notes 'The GDPR introduces new provisions to address the risks arising from profiling and automated decision-making, notably, but not limited to, privacy.' Article 29WP, Guidelines on Automated individual decision-making n 97, 6.
138 Rouvroy, n 57, 22. See also Bart van der Sloot, 'The Individual in the Big Data Era: Moving towards an Agent-based Privacy Paradigm', in Bart van der Sloot et al. (eds.), *Exploring the Boundaries of Big Data* (Amsterdam: Amsterdam University Press, 2016), 177.
139 See also Purtova, who argues that 'the material scope of . . . the GDPR, is growing so broad that the good intentions to provide the most complete protection possible are likely to backfire in a very near future, resulting in system overload.' Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 (1) *Law, Innovation and Technology*, 40, 41.
140 Rouvroy, n 57, 22.
141 Ibid.
142 The indicative list of risks that can arise from the processing of personal data provided in Recital 75 GDPR demonstrates this conflation and confusion of issues. More particularly, Recital 75 states that risks of processing of personal data include 'discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the

processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.' With the necessary caveats that 'risks' under the GDPR have a slightly different meaning from 'challenges' and 'issues' as discussed in this chapter and they do not concern big data in particular but any type of processing of personal data, Recital 75 contains a mixture of different types of risks (some concern the *processing* of personal data, some the *outcomes* of processing, some are *societal*) put together without any differentiation. This is also problematic for controllers, who are required to decide when processing is of 'high risk' or which data breaches entail such 'risks'.

143 Rouvroy, n 57, 22. Emphasis added.

144 The ICO notes 'It's not a case of big data *or* data protection, it's big data *and* data protection; the benefits of both can be delivered alongside each other.' Information Commissioner's Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, 20170904 Version: 2.2, para 28.

145 Art. 1 GDPR.

146 Commission, 'The EU Data Protection Reform and Big Data, Factsheet' March 2016. See also Gonçalves n 6, 114 who argues that the GDPR demonstrates 'the EU's deliberate, actually explicit intent to simplify rules for companies in the digital age' and 'caught between its twofold objective of strengthening the rights of the data subjects, and facilitating business, the EU legislator ended up favouring the latter to the detriment of the former.'

147 See Art. 5 (1).

148 Mayer-Schonberger and Padova, n 14, 318.

149 Zuboff, n 133, 75.

150 Art 25 GDPR and Recital 78.

151 As the EDPS correctly recommends 'Designers and manufacturers should apply the same level of creativity and dynamicity they usually display in introducing attractive devices and apps to also provide individuals with effective and user-friendly privacy notices and setting options. As a result, individuals should be able to set options relevant to their privacy and data protection with the awareness that this is an important element of the devices and apps' use, in their own personal interest, and not a boring formality or a useless burden.' EDPS, Opinion 1/2015 Mobile Health: Reconciling Technological Innovation with Data Protection, 13. See also EDPS, Opinion 7/2015 (n 3), 14.

152 Recital 98 GDPR. See also Art 40 GDPR.

153 The Centre for Information Policy Leadership (CIPL) observes that 'Despite the fact that there are six legal basis contained in the GDPR, none of which are privileged over the other, there is a general feeling among data protection practitioners, lawyers and DPOs that DPAs, lawmakers and policymakers in the EU place strong emphasis on consent as a more important legal basis . . . For the GDPR to serve as a modern privacy law, its consent requirements cannot be emphasised as the principal legal ground for processing, nor should the other legal bases be continuously construed narrowly.' Centre for Information Policy Leadership, 'GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges', 31 May 2019 <www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf>, 8.

154 Art 29 WP Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6.

155 Ibid, 19.

156 See also Recital 71.

157 Article 15 (1) (h) GDPR.
158 Articles 13 (2) (f) and 14 (2) (g) GDPR.
159 Article 22 (3) GDPR.
160 Article 4 (2) GDPR.
161 See Article 29WP, Guidelines on Automated individual decision-making n 97, 9–19.
162 Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008), 166.
163 As Koops observes 'This . . . requires stretching the concept of personal data (sometimes to the point of breaking, or perhaps rather of becoming void of meaning), or stretching the regulatory problem so that it becomes a problem of processing personal data.' Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 (4) *International Data Privacy Law*, 250, 258.
164 Ibid, 260.
165 See Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions', University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2014–8; Crawford and Schultz propose 'procedural data due process' for big data that 'rather than attempt regulation of personal data collection, use, or disclosure ex ante, procedural data due process would regulate the fairness of Big Data's analytical processes with regard to how they use personal data (or metadata derived from or associated with personal data) in any adjudicative process, including processes whereby Big Data is being used to determine attributes or categories for an individual.' Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 *B.C.L. Rev.*, 93, 109.
166 Hoffman, n 88, 85.
167 EDPS, Opinion 1/2015 *Mobile Health: Reconciling Technological Innovation with Data Protection*, 21 May 2015, 10.
168 Data brokers should comply with data protection legislation, but specific legislative measures could also be applicable to them. See Privacy International, 'Why We've Filed Complaints Against Companies that Most People Have Never Heard Of – And What Needs to Happen Next', 8 November 2018 <https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what>; Amit Katwala, 'Forget Facebook, Mysterious Data Brokers are Facing GDPR Trouble', *Wired*, 8 November 2018 <www.wired.co.uk/article/gdpr-acxiom-experian-privacy-international-data-brokers>.
169 See Christian Sandvig et al., 'An Algorithm Audit', in Seeta Peña Gangadharan (eds.), *Data and Discrimination: Collected Essays* (Washington, DC: New America Foundation, 2014). <http://www-personal.umich.edu/~csandvig/research/An%20Algorithm%20Audit.pdf>. The authors propose audits for online platforms that 'will ascertain whether algorithms result in harmful discrimination by class, race, gender, geography, or other important attributes.'
170 Solove, n 24, 1880.
1 Department of Health & Social Care, 'The Future of Healthcare: Our Vision for Digital, Data and Technology in Health and Care' (2018) <www.gov.uk/government/publications/the-future-of-healthcare-our- vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for- digital-data-and-technology-in-health-and-care>, Future Advocacy and Wellcome, 'Ethical, Social and Political Challenges of Artificial Intelligence in Health' (2018) <https://wellcome.ac.uk/sites/default/files/ai-in-health-ethical-social-political-challenges.pdf>, House of Commons Science and Technology Committee, 'Algorithms in Decision-making' (HC 351, 2018) and <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/351/351.pdf>, National Advisory Group on Health Information Technology in England, 'Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England' (2018) <www.gov.uk/government/publications/using-information-technology-to-improve-the-nhs>.

2 Department of Health and Social Care (n 1). See for example National Data Guardian, 'National Data Guardian for Health and Care 2017 Report: Impact and Influence for Patients and Service Users' (2017) <www.gov.uk/government/publications/national-data-guardian-2017-report>.
3 Department of Health and Social Care (n 1).
4 NHSx, 'Artificial Intelligence: How to Get It Right: Putting Policy into Practice for Safe Data-driven Innovation in Health and Care' (2019) <www.nhsx.nhs.uk/assets/NHSX_AI_report.pdf>, 37–39.
5 Ibid 27.
6 Luciano Floridi, 'Soft Ethics, the Governance of the Digital and the General Data Protection Regulation' (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180081, Alan F.T. Winfield and Marina Jirotka, 'Ethical Governance Is Essential to Building Trust in Robotics and Artificial Intelligence Systems' (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180085.
7 The principal bodies engaged with developing information governance policies include the Care Quality Commission, the Information Commissioner's Office, the General Medical Council, the Health Research Authority and the Medicines and Healthcare products Regulatory Agency. In addition to these organizations is another set of bodies which provide governance oversight: National Data Guardians, NHS Digital, NHS England & Improvement and the National Institute for Health and Care Excellence.
8 René von Schomberg and Europäisches Parlament (eds), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields: Presentations Made at a Workshop Hosted by the Scientific and Technological Assessment Unit of the European Parliament in November 2010* (Public Office of the European Union, 2011), British Academy & Royal Society, 'Data Management and Use: Governance in the 21st Century' (2017) <https://royalsociety.org/~/media/policy/projects/data-governance/data-management-governance.pdf>, Academy of Medical Sciences & Royal Academy of Engineering, 'Health Apps: Regulation and Quality Control' (2015) <https://acmedsci.ac.uk/file-download/37073-552cc937dcfb4.pdf>, National Data Guardian for Health and Care, 'Review of Data Security, Consent and Opt-Outs' (2016) <www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs>, House of Lords Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (HL Paper 100, 2018), ch 1–6 and Nuffield Council on Bioethics, 'Bioethics Briefing Note: Artificial Intelligence (AI) in Healthcare and Research' (2018) <http://nuffieldbioethics.org/wp-content/uploads/Artificial-Intelligence-AI-in- healthcare-and-research.pdf>.
9 It should be noted that Article 40 GDPR permits the design and use of "codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation . . . " but for specified purposes. See also Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press, 2011), chapters 2–3.
10 See for example European Data Protection Supervisor (EDPS), 'Opinion 8/2016, Coherent Enforcement of Fundamental Rights in the Age of Big Data', 23 September 2016, 'Opinion 4/2015, Towards a New Digital Ethics: Data, Dignity and Technology', September 2015 and Julia Black, 'Talking about Regulation' [1998] *Public Law* 77, 78.
11 See Recital 13 and Article 5 (2) of the General Data Protection Regulation 2016 (GDPR). Also consider Articles 24 (3), 28 (5) and 32 (3) GDPR. It should be noted that Article 40 GDPR permits the design and use of "codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation . . . " but for specified purposes. See EDPS, 'Preliminary Opinion, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', March 2014 and 'Opinion, on the Communication from the Commission on 'eHealth Action Plan 2012–2020 – Innovative healthcare for

the 21st century, 27 March 2013. See also European Commission, eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century COM (2012) 736 final.

12 Patrick Henry Winston, *Artificial Intelligence* (3rd ed, Addison-Wesley Pub Co, 1992), 5.

13 Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (2nd ed., Prentice Hall, 2003), 194.

14 Organisation for Economic Cooperation and Development, *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449* (2019).

15 Fei Jiang and others, 'Artificial Intelligence in Healthcare: Past, Present and Future' (2017) 2 *Stroke and Vascular Neurology* 230.

16 Julia Schnatz, 'NHS England's Smartphone App for Identifying Acute Kidney Injury' (2016) <www.centreforpublicimpact.org/case-study/nhs-englands-smartphone-app-identifying-acute-kidney-injury-2016-2018/> accessed 11 January 2020.

17 Scott Mayer McKinney and others, 'International Evaluation of an AI System for Breast Cancer Screening' (2020) 577 *Nature* 89, Anabik Pal and others, 'Psoriasis Skin Biopsy Image Segmentation Using Deep Convolutional Neural Network' (2018) 159 *Computer Methods and Programs in Biomedicine* 59 and Stacy M. Carter and others, 'The Ethical, Legal and Social Implications of Using Artificial Intelligence Systems in Breast Cancer Care' (2020) 49 *The Breast* 25.

18 Daniel Shu Wei Ting and others, 'Artificial Intelligence and Deep Learning in Ophthalmology' (2019) 103 *British Journal of Ophthalmology* 167.

19 Kun-Hsing Yu, Andrew L, Beam and Isaac S, Kohane, 'Artificial Intelligence in Healthcare' (2018) 2 *Nature Biomedical Engineering* 719.

20 Orlando Simpson and Sergio G. Camorlinga, 'A Framework to Study the Emergence of Non-Communicable Diseases' (2017) 114 *Procedia Computer Science* 116, Abrar Alturkistani and others, 'Health Information Technology Uses for Primary Prevention in Preventive Medicine: A Scoping Review Protocol' (2018) 8 *BMJ Open* e023428 and François Bastardot and David Gachoud, 'Visual Diagnosis: Between Medical Education and Advances in Artificial Intelligence' (2019) 15 *Revue Medicale Suisse* 2145. <www.sciencedirect.com/science/article/pii/S1877050917318203> accessed 11 January 2020. See also Department of Health and Social Care, 'Prevention is better than cure' (2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/753688/Prevention_is_better_than_cure_5-11.pdf> 12–13.

21 Andre Esteva and others, 'Dermatologist-Level Classification of Skin Cancer with Deep Neural Networks' (2017) 542 *Nature* 115.

22 Abrar Alturkistani and others, 'Health Information Technology Uses for Primary Prevention in Preventive Medicine: A Scoping Review Protocol' (n 20) and François Bastardot and David Gachoud, 'Visual Diagnosis: Between Medical Education and Advances in Artificial Intelligence' (n 20).

23 Geraldine M. Clarke and others, 'Evaluating the Impact of Healthcare Interventions Using Routine Data' (2019) 365 *BMJ*.

24 Gary Marcus and Ernest Davis, *Rebooting AI: Building Artificial Intelligence We Can Trust* (First edition, Pantheon Books, 2019), 5–10. Royal Society, 'Digital Healthcare: The Impact of Information and Communication Technologies on Health and Healthcare' (2006), Ch 4.

25 D. Warner, J. Sale and E. Viirre, 'Distributed Medical Intelligence. A Systems Approach for Developing and Integrative Health Care Information Distribution Infrastructure' (1996) 29 *Studies in Health Technology and Informatics* 80.

26 Tim K. Mackey and others, '"Fit-for-Purpose?" – Challenges and Opportunities for Applications of Blockchain Technology in the Future of Healthcare' (2019) 17 *BMC Medicine* 68, Gary Leeming, James Cunningham and John Ainsworth, 'A Ledger of Me: Personalizing Healthcare Using Blockchain Technology' (2019) 6 *Frontiers in Medicine* 171 and Dee Luo and others, 'Mobile Apps for Individuals With Rheumatoid

Arthritis: A Systematic Review' (2019) 25 *Journal of Clinical Rheumatology: Practical Reports on Rheumatic & Musculoskeletal Diseases* 133.

27 Naomi J. Fulop and Angus I.G. Ramsay, 'How Organisations Contribute to Improving the Quality of Healthcare' (2019) 365 *BMJ*.

28 David J. Duffy, 'Problems, Challenges and Promises: Perspectives on Precision Medicine' (2016) 17 *Briefings in Bioinformatics* 494 and Aisling McMahon, Alena Buyx and Barbara Prainsack, 'Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond' [2019] *Medical Law Review* 1, 2–5.

29 Cameron Holley, Neil Gunningham and Clifford D. Shearing, *The New Environmental Governance* (Earthscan, 2012), 4–7.

30 Department of Health and Social Care, *The Future of Healthcare: Our Vision for Digital, Data and Technology in Health and Care* (n 1).

31 EDPS, 'A Preliminary Opinion on Data Protection and Scientific Research', 6 January 2020.

32 See Lon Fuller, *The Morality of Law* (Yale University Press; Revised edition, 1977), 106. See also EDPS, 'Opinion 5/2018 Preliminary Opinion on Privacy by Design', 31 May 2018, 10 and EDPS 'Opinion 7/2015, Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability', 19 November 2015, 16–17.

33 EDPS, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation' (v1.9 July 2019), 5.

34 Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015), Ch 3 and Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014), Ch 2.

35 Claudia Martínez Imogen Farhan, 'Making the Right Choices: Using Data-driven Technology to Transform Mental Healthcare' (2018) <https://reform.co.uk/index.php/research/data-driven-healthcare-regulation-regulators>, 31–39.

36 Academy of Royal Medical Colleges, 'Artificial Intelligence in Healthcare' (2019) 23.

37 NHSx, 'Artificial Intelligence: How to Get It Right Putting Policy into Practice for Safe Data-driven Innovation in Health and Care' (n 4) 28–36.

38 EDPS, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation' (n 33) 5.

39 European Data Protection Board, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, adopted 12 February 2019, para 7.

40 Julia Black, 'Talking about Regulation' (1998) *Public Law* 77, 77.

41 Tony Prosser, *The Regulatory Enterprise: Government, Regulation, and Legitimacy* (OUP, 2010), 2–3.

42 See for example ECtHR, I v Finland, No. 20511/03, 17 July 2008, paragraph 38 and ECHR 25 November 2008, 2010] ECHR 2229, 36919/02, paragraph 40.

43 See, for example, EDPS Opinion on the Commission proposals for a Regulation on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and a Regulation on in vitro diagnostic medical devices, 8 February 2013, para 4–13. Also see Article 29 Working Party, 'Opinion on Apps on Smart Devices', adopted 27 February 2013 (WP 202).

44 See Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor", adopted on 16 February 2010 (WP 169).

45 Menno Mostert et al., 'From Privacy to Data Protection in the EU: Implications for Big Data Health Research' (2017) 25 (1) *European Journal of Health Law* 43, 44.

46 It is beyond the scope of this chapter to assess if the appropriate balance has been struck.

47 See EDPS, 'Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free-Flow of Non-Personal Data in the European Union', 8 June 2018 <https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-framework-free-flow-non-personal-data_en>,

2–6. Also Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) *Law, Innovation and Technology* 10 (1) 40–81 Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2016) *Seton Hall L. Rev* 47 and Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 (2) *Computer Law & Security Review* 279–288.

48 Boston Consulting Group, 'The Value of our Digital Identity' (2012) <www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>.

49 Michael Phillips and others, 'Assessment of Accuracy of an Artificial Intelligence Algorithm to Detect Melanoma in Images of Skin Lesions' (2019) 2 *JAMA Network Open* e1913436.

50 See also Recital 35 GDPR.

51 Recital 26 GDPR.

52 Article 4 (5) and Recital 26 GDPR. Miranda Mourby and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 *Computer Law & Security Review* 222.

53 Nadezhda Purtova, 'Property Rights in Personal Data: Learning from the American Discourse' (2009) 25 (6) *Computer Law & Security Review* 507–521.

54 For identifiability and dynamic IP addresses, see CJEU, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 19 October 2016. Also observations in CJEU, C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24 November 2011 para 51.

55 ECtHR, Szuluk v the United Kingdom, No. 36936/05, 2 June 2009 and 'Letter from Chair of Article 29 Working Party on New Draft Code of Conduct', 11 April 2018 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=625391>.

56 Giovanni Comandè and Giulia Schneider, 'Regulatory Challenges of Data Mining Practices: The Case of the Never-Ending Lifecycles of "Health Data"' (2018) 25 *European Journal of Health Law* 284 and OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (2015) <www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en>.

57 See Jaap-Henk Hoepman, 'Privacy Design Strategies (The Little Blue Book)' (2019) <www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>.

58 European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM (2018) 233. See Simon Woods, 'Big Data Governance: Solidarity and the Patient Voice' in Brent Daniel Mittelstadt and Luciano Floridi (eds), *The Ethics of Biomedical Big Data* (Springer, 2016), 221–238 and Annemarie Mol, *The Logic of Care. Health and the Problem of Patient Choice* (Routledge, 2008) who argues how regulations frame choices and create the impression of autonomy and freedom.

59 See CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [GC], 9 November 2010, para 48 and Alvin Liu, 'Smartphone-Based, Artificial Intelligence – Enabled Diabetic Retinopathy Screening' (2019) 137 *JAMA Ophthalmology* 1188.

60 See EDPS, 'Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' 19 December 2019, 6–12.

61 Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague, Kluwer Law International, 2002), 50–52. See also CJEU, C-543/09, Deutsche Telekom AG v. Bundesrepublik Deutschland, 5 May 2011, para 51–52 on the balancing requirements.

62 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014, para. 38.

63 CJEU, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy [GC], 16 December 2008, para 54–56. Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation', adopted on 2 April 2013 (WP 203) para 45–47 and

'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', adopted on 9 April 2014 (WP 217) para 9–11.

64 Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679', 3 October 2017 (WP 251) 4.

65 CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, para 88 and Article 29 Working Party, 'Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, (WP 225).

66 Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, 2017).

67 See Article 29 Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', adopted 30 May 2014 3–4 and EDPB-EDPS, 'Joint Opinion 1/2019 on the Processing of Patients' Data and the Role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)' (2019) <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12019-processing_en>.

68 The satisfaction of the legal basis requirement does not absolve data controllers from fulfilling other obligations, such as those set out in Article 5: See Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP203), 15–16.

69 Article 9 (2)(c) GDPR.

70 Article 9 (2) (h) GDPR.

71 Article 9 (2)(i) GDPR. However see Mary Donnelly and Maeve McDonagh, 'Health Research, Consent and the GDPR Exemption' (2019) 26 *European Journal of Health Law* 97 does not take sufficient account of the contextual nature of problem solving and the risk-based approach which underpins data protection law.

72 It is important to reiterate that under the GDPR, explicit consent is only one lawful basis for processing. Additionally, Recital 26 for anonymous data.

73 As an example, see the information standard DCB3058 Compliance with National Data Opt-outs in light of section 250 of the Health and Social Care Act 2012.

74 Charlotte Bagger Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 (4) *International Data Privacy Law* 239–248, Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights? (2014) *Common Law Market Review* 51, 843–868, Christopher Docksey, 'Four Fundamental Rights: Finding the Balance' (2016) 6 International Data Privacy Law 2, Irene Kamara and Paul De Hert, 'Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground. A Pragmatic Approach', in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (CUP, 2018) and Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-making and Profiling' (2018) 34 (2) *Comp Law Sec Rev* 398, See Joined cases C-468/10 and C-469/10, ASNEF, ECLI:EU:C:2011:777, paras. 28–29, Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk, ECLI:EU:C:2003:294, paras. 17–21, C-275/06, Promusicae, ECLI:EU:C:2008:54, paras. 29–33. C-73/07, Satamedia, ECLI:EU:C:2008:727, paras. 25–26. Joined Cases C-92/09 and C-93/09, Schecke, ECLI:EU:C:2010:662, paras. 26–29. Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238, paras. 17 and 20. Also EDPS, 'Developing a Toolkit for Assessing the Necessity of Measures that Interfere with Fundamental Rights', 11 April 2017 <https://edps.europa.eu/sites/ edp/files/publication/16–06–16_necessity_paper_for_consultation_en.pdf>, 4–6.

75 EDPS, 'Opinion 1/2015 Mobile Health Reconciling Technological Innovation with Data Protection', 21 May 2015 para 57.

76 ibid. para 55–63.

77 Article 12 (1) GDPR.
78 Articles 13 and 14 GDPR.
79 Article 15 GDPR.
80 Article 16 GDPR.
81 Article 17 GDPR.
82 Article 21 GDPR.
83 Article 22 GDPR.
84 OECD, 'Recommendation of the Council on Health Data Governance', OECD/LEGAL/0433, Pratik Shah and others, 'Artificial Intelligence and Machine Learning in Clinical Development: A Translational Perspective' (2019) 2 *Digital Medicine* 1 <www.nature.com/articles/s41746-019-0148-3> accessed 11 January 2020.
85 Trishan Panch and others, 'Artificial Intelligence: Opportunities and Risks for Public Health' (2019) 1 *The Lancet Digital Health* e13 <www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30002-0/abstract> accessed 11 January 2020. Viet-Thi Tran, Carolina Riveros and Philippe Ravaud, 'Patients' Views of Wearable Devices and AI in Healthcare: Findings from the ComPaRe e-Cohort' (2019) 2 *Digital Medicine* 1 <www.nature.com/articles/s41746-019-0132-y> accessed 11 January 2020.
86 NHSx, 'Artificial Intelligence: How to Get it Right: Putting Policy into Practice for Safe Data-driven Innovation in Health and Care' (n 4) 17 and Ryan Poplin and others, 'Prediction of Cardiovascular Risk Factors from Retinal Fundus Photographs via Deep Learning' (2018) 2 *Nature Biomedical Engineering* 158–164.
87 EDPS, Meeting the Challenges of big data, Opinion 7/2015 (n 32) and European Data Protection Supervisor (2016), Coherent enforcement of fundamental rights in the age of Big Data, Opinion 8/2016 (n 10) and Kun-Hsing Yu, Andrew L. Beam and Isaac S. Kohane, 'Artificial Intelligence in Healthcare' (2018) *Nature Biomedical Engineering* 2, 719–731.
88 Michael V. Hayes, 'On the Epistemology of Risk: Language, Logic and Social Science' (1992) 35 *Social Science & Medicine* 401, Michael Snyder and Wenyu Zhou, 'Big Data and Health' (2019) 1 *The Lancet Digital Health* e252, Jessica Morley, Mariarosaria Taddeo and Luciano Floridi, 'Google Health and the NHS: Overcoming the Trust Deficit' (2019) 1 *The Lancet Digital Health* e389 and Mariarosaria Taddeo, 'Modelling Trust in Artificial Agents, A First Step Toward the Analysis of e-Trust' (2010) 20 *Minds and Machines* 243 <http://link.springer.com/10.1007/s11023-010-9201-3>.
89 Saskia Hendriks and others, 'Ethical Challenges of Risk, Informed Consent, and Post-trial Responsibilities in Human Research With Neural Devices: A Review' (2019) 76 *JAMA Neurology* 1506.
90 Aisling McMahon, Alena Buyx and Barbara Prainsack, 'Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond' (n 28) 8 and Filippo Pesapane and others, 'Artificial Intelligence as a Medical Device in Radiology: Ethical and Regulatory Issues in Europe and the United States' (2018) 9 *Insights into Imaging* 745.
91 Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law* 3.
92 Luciano Floridi, 'Soft Ethics, the Governance of the Digital and the General Data Protection Regulation' (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180081, Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 *European Journal of Risk Regulation* 502 and Michael Snyder and Wenyu Zhou, 'Big Data and Health' (2019) 1 *The Lancet Digital Health* e252. See also European Parliament and the Council of the European Union, Regulation (EU) 2017/745 of the European Parliament and of the Council 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, Official Journal of the European Communities (2017) and European Parliament and the Council of the European Union Regulation (EU) 2017/746 of the European parliament and of the Council on in vitro diagnostic medical devices and repealing directive 98/79/EC and commission decision 2010/227/EU, Official Journal of the European Communities (2017).

93 European Data Protection Supervisor (2019), 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation' (n 33).

94 Lee A. Bygrave, *Data Protection Law – Approaching Its Rationale, Logic, and Its Limits* (Kluwer, 2002), 3–15, Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law* 3.

95 Ibid.

96 European Data Protection Board, 'Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom Regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)', 25 September 2018). It endorses Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (WP 248). See also Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk – Understanding Risk Regulation Regimes* (Oxford University Press, 2001), 3. They suggest that governance involves three interacting elements: standard-setting, information-gathering and behaviour-modification.

97 Article 35 (7) GDPR.

98 Article 35 (3) (a) (b) GDPR.

99 Roger Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (2011) 1 *International Data Privacy Law* 111.

100 European Data Protection Board endorses Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) 9–11.

101 See Article 36 GDPR.

102 Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679' (n 95). See critique Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 *International Data Privacy Law* 22.

103 Athena Bourka and others, 'Recommendations on Shaping Technology According to GDPR Provisions: Exploring the Notion of Data Protection by Default' (2018) <http://dx.publications.europa.eu/10.2824/518496> accessed 9 January 2020. Henry Rothstein and others, 'The Risks of Risk-Based Regulation: Insights from the Environmental Policy Domain' (2006) 32 *Environment International* 1056, 1057. The Royal Society, *Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis* (The Royal Society, 2019), 1, Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 (2) *Oslo Law Review* 105–120.

104 Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 *International Journal of Law and Information Technology* 151, Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International Data Privacy Law* 105, Mélanie Bourassa Forcier and others, 'Integrating Artificial Intelligence into Health Care through Data Access: Can the GDPR Act as a Beacon for Policymakers?' (2019) 6 *Journal of Law and the Biosciences* 317.

105 Royal Society Working Group, 'Machine Learning: The Power and Promise of Computers that Learn by Example' (2017) <https://royalsociety.org/-/media/policy/projects/machine-learning/publications/machine-learning-report.pdf> and Sicco Verwer and Toon Calders, 'Introducing Positive Discrimination in Predictive Models', in Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky (eds), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer, 2013), 255–270.

106 Isak Mendoza and Lee Bygrave, 'The Right Not to be Subject to Automated Decisions based on Profiling', in Tatiani Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou (eds), *EU Internet Law: Regulation and Enforcement* (Springer, 2017), 77–98 and Sandra Wachter and Mittelstadt Brent, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) *Columbia Business Law Review*, 495.

107 Nicholas Diakopoulos and others, 'Principles for Accountable Algorithms and a Social Impact Statement for Algorithms' (nd) <www.fatml.org/resources/principles-for- accountable-algorithms>.

108 Dillon Reisman, Jason Schultz, Kate Crawford and Meredith Whittaker, 'Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability' (2018) <https://ainowinstitute.org /aiareport2018.pdf>.

109 Sharon Vallor, 'An Ethical Toolkit for Engineering/Design Practice' (2018) <www.scu.edu/ethics-in-technology-practice/ethical-toolkit/>.

110 Department of Health and Social Care, 'NHS Constitution for England' (2015) <www.gov.uk/government/publications/the-nhs-constitution-for-england>.

111 See National Information Board, 'Framework for Action' Entitled Personalised Health and Care 2020: Using Data and Technology to Transform Outcomes for Patients and Citizens' (2014) <www.gov.uk/government/publications/personalised-health-and-care-2020>.

112 See for example, Department for Business, Innovation and Skills, 'Better Regulation Delivery Office, Regulators' Code' (2014) <www.gov.uk/government/publications/regulators-code> and sections 21 and s22 of the Legislative and Regulatory Reform Act 2006.

113 AHSN Network, 'Accelerating Artificial Intelligence in Health and Care: Results from a State of the Nation Survey' (2018) <www.ahsnnetwork.com/> 7.

114 Department for Digital, Culture, Media & Sport, 'Data Ethics Framework' (2018) <www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework>.

115 See for example, Health Research Authority and the UK Health Departments, 'UK Policy Framework for Health and Social Care Research' (2017) </planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/>. Where identifiable sensitive personal data is used data protection rules on lawful basis must be complied with. Additionally, the provisions under section 251 of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002 must be complied with. For AI based medical devices, the Medical Devices (Amendment etc.) (EU Exit) Regulations 2019 should be complied with in addition to fulfilling the guidance provided by the Medicines and Healthcare products Regulatory Agency.

116 NHS Digital, 'Data Security and Protection Toolkit' (2018) <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit>.

117 See Section 250 Health and Social Care Act 2012 definition of standards and DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems. The UK Caldicott Guardian Council provides regulatory oversight with regard to the protection and use of sensitive personal information of individuals when providing health and care services.

118 Julia Black, 'Paradoxes and Failures: "New Governance" Techniques and the Financial Crisis' (2012) 75 *The Modern Law Review* 1037.

119 Principle 1 Code of Conduct.

120 Principle 2 Code of Conduct.

121 Graeme Laurie and Nayha Sethi, 'Towards Principles – Based Approaches to Governance of Health – Related Research Using Personal Data' (2013) 4 *European Journal of Risk Regulation* 43.

122 Principle 9 Code of Conduct.