**COMMISSION ON *GOVERNING HEALTH FUTURES 2030:***
**RESPONSE BY NICK COULDRY (LSE) AND ULISES A. MEJIAS (SUNY OSWEGO)**

*Introduction*

1.1 Health is a fundamental dimension of life: a human being's health is the matrix of factors which determine whether her life is sustained. Health data are therefore among the most personally significant data about a person. For that reason, the principle of patient confidentiality has been at the core of medical ethics for more than two millennia.[1] But every sector of life today is being transformed by the social process of "datafication": that is, the conversion of the flow of life into data, leading to unprecedented new forms of collecting, storing, processing and exchange data, and the emergence of many new actors with stakes in such data. Health, a sector of great economic and public value, is no exception: corporations and governments around the world are hugely interested in the production of health data. But can datafication in the health sector be managed in ways that respect individual rights and safeguard populations against negative social externalities? That is highly uncertain.

1.2 Human beings have not only a right to life, but a right to control over the flow of information about their life. For this reason, the UN Human Rights Commissioner Michele Bachelet has stated that the "digital revolution" (of which datafication "on an industrial scale" is unmistakably part) "is a major global human rights issue".[2] The right to control over personal information flows from Article 22 of the Universal Declaration of Human Rights under which "everyone, as a member of society . . . is entitled to realization . . . of the economic, social and cultural rights indispensable for his dignity and the free development of his personality". The principle of "the free development of [an individual's] personality" is echoed in Article 2.1 of the German constitution, on which German courts have reflected in detail, linking it to a general "right to informational self-determination".[3]

1.3 Data about a person's health – and the narratives about their state of health, propensity to illness, life expectation, and so on, that can be generated from such data – are highly consequential to that person's life. Each person's right to control the information produced and circulated about their health is therefore a fundamental aspect of her personal integrity. Respect for the sensitivity of health data is a core component of respecting a person *as* a person. But the right of

individuals to protection of their health data is not currently recognised sufficiently in debates about the production and management of data in the health sector.

1.4 Although data rights are generally discussed in terms of the rights of individuals, the uneven group distribution of both health risks and data harms means that there may be specific groups of people who are particularly exposed to harm through lack of protection of their health data: for example, those with chronic health problems, those with a disability, ethnic groups with higher disease exposure, older cohorts and, more generally, those living in societies which have weak negotiating power in relation to the management of health resources and/or the provision of the computing infrastructure necessary for the management of health data. We return to this issue later in the paper when we consider longer-term trends.

1.5 Meanwhile the science of health (medicine) requires the production, aggregation and analysis of health data. The more contextually rich such data is, the more scientifically useful it may be. Recent advances in data gathering, data storage, and data processing make possible medical research on a scale and depth and at speeds without historical precedent: new forms of health-related data are also being gathered through various forms of "self-tracking". The potential benefits for medical knowledge are huge, but the potential social risks of datafication in the health sector are also huge. As a result, contemporary societies face a problem: *how to calibrate potential scientific benefits from the vast growth in health data with the potential social risks of managing such data without due regard to individuals', families' and communities' rights to personal protection?* The fast growth in datafication across every sector of society today, and in every region of the world, makes such calibration particularly difficult both to conceptualize and to implement.

1.6 Calibrating the scientific benefits from the flow of health data to its potential social risks is the aspect of *Governing Health Futures* on which this short paper focuses.

*Background*

2.1 The implications for human rights protection of flows of personal data has increasingly been recognised by the world's legal systems. As the opening of the European Union's General Data Protection Regulations (GDPR) puts it, "the protection of natural persons in relation to the processing of personal data is a fundamental right".[4] A similar principle has been adopted in legislatures around the world (including India, Japan, Australia, Canada, the United Kingdom and the

US state of California). That right applies to health data just as much as to any other type of personal data.

2.2 The GDPR has special provisions dealing with health data, clarifying for regulatory purposes 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".[5] The possibility of special provisions permitting the processing for reasons of public health of "certain categories of personal data without the consent of the data subject" is noted,[6] but the right of EU member states to pass additional protective legislation relating to "the processing of genetic data, biometric data or data concerning health" is also recognised.[7] It is clear therefore that, as the world's leading legal framework for the protection of personal data, the GDPR recognises the special importance of health data, while acknowledging the special challenges of public health emergencies (which we discuss in the context of COVID-19 at the end of this document).

2.3 Leaving aside health data flows directly necessary to combat public health emergencies, there are general pressures towards maximising the production and circulation of health data. Health data is potentially beneficial, for example, for the identification of diseases, for tracking the spread of disease, and for researching possible cures against disease. Because of the personal importance of health data, there are, in most legislatures across the world, general legal and professional restrictions on the release of personally identifying health data without the consent of the person to whom that data relates. But the factors shaping *whether* a person consents to release or exchange of their health data, for example for the purposes of medical research, are multiple, and risk introducing a "consent bias" to health datasets which distorts scientific outcomes.[8] For that reason, some medical legal scholars argue for broader powers for the collection and circulation of health data not limited by the obtaining of specific patient consent.[9] It is certainly possible to envisage particular societies evolving social contracts whereby health data is collected, exchanged and processed on a large scale, overriding individual rights to refuse consent, on the basis of an agreed collective purpose (e.g. to support research towards the cure of a certain type of cancer that affects a distinct profile of the population). It follows that, even outside the case of public health emergencies, there is a need for debate about the conditions under which personal

rights to control the flow of personal health data should be either respected or sometimes limited.

2.4 That said, the recent growth of the health data sector, within and beyond the medical profession, is creating wider economic and social pressures for a general market in health data that far exceeds the scope of any specific "social contracts" for gathering personal health data that we might imagine. The challenge therefore is to evaluate the risks of that health data market being allowed to expand without constraint and without regard to its social externalities. It is particularly important to identify the social externalities that will result when flows of personal health data are stimulated outside the two types of restricted circumstances under which personal health data has until now been expected to flow: (a) within the ambit of the confidential doctor-patient relationship and (b) for exceptional reasons of public health emergency.

2.5 As with any form of personal data, the meaning of health data changes depending on whose hands it falls into. Data on a person's life expectancy means one thing to a doctor concerned with sustaining that person's life or reducing the risks to a population from the defined health risks with which that person presents, and it means quite another thing to an insurer concerned to limit the commercial costs of a policy by identifying exclusions to that policy. Insurers are only the most obvious example of *a non-medical actor* that has an interest in getting access to personal health information. Providers of personal finance are interested in accessing personal health data which may help in assessing a potential borrower's life expectancy or the risks that their earning capacity might be curtailed. State providers of welfare payments will have similar interests in accessing personal health data. Marketers, in a more diffuse way, may be able to benefit from health and much other personal data. In multiple ways, therefore the unrestricted circulation of personal health data creates new opportunities for *managing populations* which, by the same token, create risks of *unequal power relations*. At a broad social scale, there emerges the risk of a digital welfare state that is driven "to automate, predict, identify, surveil, detect, target and punish", as the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, put it recently.[10] Risks from the collection of health data combine with risks of making automated decisions based on such data, leading to a process of what US sociologist Virginia Eubanks calls "automating inequality".[11]

2.6 Before we consider in more detail the potential social externalities that derive from the unrestricted gathering and use of health data, these developments need to be placed in the larger context of societal development, of which datafication in the health sector is just one part. In the past five years, there has been much debate amongst social scientists about what practices for the collection of personal data on a vast scale - in every sector from marketing to personal finance, education to health, government to global development - mean. There is widespread consensus that they represent a significant development in global capitalism. Without question, digital information has become massively more significant in economic production over the last three decades. So too have activities and transactions across the internet, accessed particularly via mobile phones, with the result that dependence on online services for much of everyday life is far advanced.

2.7 Sociologist Shoshana Zuboff argues that overriding these general trends is a new form of exploitation based on the extraction of economic value from the data generated by many aspects of human life online, what she calls "surveillance assets" within her wider thesis of "Surveillance Capitalism". Yet, on the face of it, data gathered as part of relations between doctor and patient are not "surveillance assets", because a doctor's care for their patient is not regarded by anyone as external surveillance, but rather as observation and data gathering that is necessary for that relationship of care. But, as Zuboff notes and as noted earlier (paragraph 1.4),[12] the domain of *potential* health data is expanding hugely through forms of digital tracking to which individuals consent as part of their everyday life (such as Fitbit and Apple Watch). The voluntary wearing of such health monitoring devices generates health-*related* data whose processing may not be subject to the same legal restrictions as health data proper. The generation of such data is being stimulated for example by employers in return for offers of work-related health insurance, and the providers of such apps and devices are forging alliances with health insurers. A wider nexus of health-related data collection is therefore emerging which may fit the wider pattern of surveillance capitalism. More broadly, this trend can be seen as part of a new colonial stage of capitalism ("data colonialism") in which, in an echo of the historic colonial land-grab of resources that made capitalism originally possible, human life itself is becoming the new target of economic extraction.[13] The frameworks of surveillance capitalism and data colonialism point to much larger risks from the growth of health data, which

only reinforce the need to review the personal and social protections that are in place here.

2.8 The analysis that follows however does not depend on acceptance of the broader theses of surveillance capitalism and/or data colonialism. The potential social externalities from health data flows will in what follows be analysed at three levels - basic risks, resulting power dynamics, and wider societal risks – followed by a separate note on implications of the COVID-19 crisis.

*Basic risks*

3. In this section we identify some basic risks of social harm that are liable to arise given the intrinsic sensitivity of health data, and the new circumstances in which health data is being generated today.

3.1 Even where data is being gathered and stored within the context of a confidential doctor-patient relationship, the sheer volume of health data collection today raises issues. Since all data must be stored, the storage requirements for a medical practice's patient data are likely to exceed the secure storage capacity of that practice's computers; larger storage issues will arise at the level of hospitals or regional health systems. Storage will therefore come to depend, if it does not already, on cloud computing, that is, shared servers in corporate hands from which medical practitioners lease storage rights. Clear rules are needed to ensure that such data storage remains under medical control and within the parameters of relevant confidentiality obligations.

3.2 There is some health data so personally sensitive that its storage should itself be allowed only under special conditions. This includes the data that comprises the genome of an individual. As philosopher Daniel Sulmasy argues,[14] the risk of abusing such data and using it against the interests of that individual are so great that special rules are needed for its storage. The GDPR alludes to this category of data,[15] but without indicating the need for any special treatment. There may be other genetic data relating to individuals that requires similar levels of extraordinary protection. Any such health data of high sensitivity should under no circumstances be transferred between entities, except for the purpose of clear and agreed medical procedures. Even in such cases, strict rules will be needed to avoid relying on patient consent in circumstances where no patient is in a position fully to appreciate the consequences of giving such consent. In short, health data of

special sensitivity should, where possible, not be stored anywhere, because of the risks of its disappearance and abuse.

3.3 A common assumption in the health sector is that personal health data should only move beyond the secure setting of a confidential doctor-patient relationship when it has been securely anonymized. A related assumption is that such anonymization is reliable.[16] But this second assumption is not secure: as a number of US medical legal scholars point out, anonymized health data can, *when combined with other data*, yield the identity of the person.[17] The general risk of de-anonymization is recognised by the GDPR, as reflected in the following passage: "the principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person".[18] The costs of de-anonymization of such highly personal data, such as health data, are potentially severe. Since the risk of de-anonymization arises not from data itself, but from its combination with other data sources, it is particularly important that *limits on the transfer and aggregation* of health and health-related data to/by data controllers (whether single actors or distributed networks) should be imposed. Serious consideration is therefore needed to restrict the exchange of health data unless and until risks of de-anonymization can be mitigated.

3.4 A specific version of the general risk of de-anonymization arises when anonymous health data is transferred between contexts (eg from a patient-doctor relationship) to a general therapeutic relationship or to another context (self-improvement, employment, commercial services). The progressive risks of de-anonymization accumulate, as data is transferred between more and more contexts. Yet the "seamless" flow of health data, as other data, is often proposed as an ideal for business. Seamless data flow should never be proposed as a norm in the health sector without first establishing that secure protection against possibilities of de-anonymization are in place.

3.5 The above risks are magnified in relation to health-*related* data, generated for example by self-monitoring devices or apps. Such data is not normally protected by general rules affecting health data confidentiality, and is regulated only by the corporate terms and conditions imposed by the provider of the app or device as a

condition of its use. As research has shown,[19] such terms and conditions very often permit implicitly much wider sharing of the data collected to commercial third parties. The combination of health and health-related data raises particular concerns: personal social data or location data (highly identifying) is often collected by health apps. When (as is likely) it is combined with health-related data, the result is likely to be a data cluster that effectively identifies the subject, even if it is formally anonymized. Such data sharing to third parties may nonetheless be permissible under the terms of even strong data protection legislation such as the GDPR if formal "consent" by the data subject can be shown. A serious question arises: what makes "consent" meaningful here, and what if there is no possibility of meaningful consent?[20]

3.6 To address the broader risks identified in 3.5, more robust rules are needed to ensure: (1) rules to enforce transparency of any practices of third-party transfer of health or health-related data beyond those strictly necessary for the functioning of a device; (2) restrictions on powerful actors imposing or strongly incentivising adoption by others (for example, employees) of a health self-tracking device that effectively impose that device's terms and conditions of data collection on its users; and (3) severe restrictions on the gathering of locational and other social data by self-tracking decides and apps whose purported purpose is health enhancement.

3.7 Estonia is often discussed as a case study of a comprehensive approach to the storage of personal data that attempts to address some of the issues identified above. Most government functions—including education, taxes, justice, voting and health care—are highly integrated into a decentralized and secure government platform called X-Road. The success of X-Road is probably tied to the fact that 99% of households in Estonia have broadband, and that computer literacy is part of the educational curriculum from an early age. But this only serves to highlight the point that this success is not so much a function of the technology being used (which is not out of reach for most countries), but of the values and priorities behind its implementation. It is the state, not the private sector, that assumes the responsibility for designing and implementing a network that increases efficiency, and this efficiency is oriented towards social benefit, not profitability. Additionally, the state assumes the responsibility of keeping the data private and secure. To say that citizens own their data in Estonia is not just marketing rhetoric; every time an agency or third party looks at a record, the activity is logged, and accessing

data without a valid reason has legal repercussions. Agreeing to share one's health data can thus result in concrete benefits, such as patients never having to file a form when visiting a doctor's office, or doctors being able to identify dangerous interactions when issuing drug prescriptions, or emergency medical technicians being able to access a person's health records even before they enter an ambulance.[21] But the conditions under which this socialized version of health data collection have been implemented are highly untypical of those prevailing in other countries across the world.

*Emerging power dynamics in the health data sector*

4. In the previous section we examined the basic risks to human rights from the collection and processing of health and health-related data. We made proposals for legal rules to limit those risks. Such rules may or may not be successfully implemented in various legislatures. Even if they are, the result may not be to halt the very powerful commercial forces currently driving the expansion of the health data sector. In this section we consider the implications if that sector continues to grow as currently seems likely.

4.1 The growth of the health data sector is assumed as a positive element in the "European strategy for data" recently published for consultation by the European Commission. This strategy singles out "personalized medicine" as one area where "data will reshape the way we produce, consumer and live", predicting the emergence of health as one "common data space" at a European level based on the free circulation of health including "genomic information".[22] A related White Paper includes health as one area for pushing forward an "Adopt AI" programme:[23] while the paper certainly recognizes the risks for society of conducting AI badly, it pays little or no attention to the social externalities of embedding AI in many sectors of everyday life.[24] Similar policies for encouraging the growth of AI, and the data collection and data exchange that it requires, in health and other sectors, have been adopted in other countries.[25]

4.2 There is evidence also of major commercial pressures for the expansion of AI in the health sector, with all the pressure to collect and circulate personal health data that inevitably flow from this. Google is a leading global player in AI, and its attempts to secure deals for data with health authorities have attracted attention, for example, in the USA and UK. In the USA Google's "Project Nightingale"

received critical attention because of its deal with the USA's second largest health system, Ascension, to move its data onto Google's cloud computing system, and thereby give Google access to all that system's data. While Google contends that the deal complies with US legislation for the portability of health data (the Health Insurance Portability and Accountability Act 1996, HIPAA), others including the Office for Civil Rights in the US Department of Health and Human Services are concerned. According to the Wall Street Journal, Google's goal is to secure access "to a 'layer' of patient information that is essentially an entire personal health record", as the basis for AI-based evaluation of health outcomes.[26] Amazon, Apple and Microsoft are other Big Tech companies with strong ambitions in the health data sector. We must wait to see how such plans evolve.

4.3 The deeper logic behind such corporate attempts to extend access to personal health data was exposed in a separate Wall Street Journal report on Google's purchase of Fitbit for US$2.1 billion announced in early November 2019. Fitbit itself was already involved in deals with chemical companies and other medical suppliers to supply data. Access to Google's AI capacity will transform Fitbit's operations while access to Fitbit's individual health and health-related data is a major asset for Google. Following the closure of Google Health in 2011, the acquisition of the US's second largest health-tracking device maker represents an important alternative strategy for Google's collection of health data. The Wall Street Journal's analysis is interesting: "health services remains an open frontier [ie for data collection] . . . Fitbit . . . cuts out the middleman [for data collection]", for example hospitals and doctors.[27] Other ways of removing obstacles to the direct collection of personal health data include plans by pharmaceutical companies for "smart pills containing miniaturized computer chips to track patient health with the data transmitted back to doctors by 5G".[28] The wider logic – first, of maximizing the collection of health and health-related data and, second, of removing so far as possible obstacles to the aggregation of such data in the hands of the largest commercial actors for data storage and data analytics – is clear.

4.4 It is reasonable from this to anticipate that a new health data infrastructure will emerge, bound together by alliances between the large players in the health sector (doctors' networks, regional health provision systems, device providers, Big Tech providers of cloud services and AI analytics, health insurers). The establishment of this infrastructure – first of all, in the most economically developed countries

(such as the USA) but potentially exportable to many other more or less economically developed countries - will serve to further normalize large-scale data collection and exchange as a basic feature of health care. That, in turn, will reduce the power of individual patients to resist such trends or get access to effective alternatives. In so far as privacy-protection options are available within this transformed health infrastructure, they are likely only to be available at a price to those who can afford that privacy "premium". Less wealthy patients, unable to pay this premium, will have to accept default settings which, without significant legal intervention, are unlikely to weigh privacy protection above the commercial benefits of unrestricted data collection and circulation. Any room for manoeuvre by individual patients will be limited by the actions of health insurers who have the power effectively to compel policyholders to accept existing terms of data processing.

4.5 In so far as players external to the health sector (from employers to governments and providers of welfare) work to endorse this growth in health data, its social influence will increase. It remains to be seen whether governments will give any priority to privacy concerns as they seek, in broad terms, to "harness" AI for assumed public health and fiscal benefits. For this reason, clear signals to governments on what data practices are and are not acceptable to protect basic human rights are all the more important. Without those signals, the forces of surveillance capitalism and data colonialism are likely to advance unchecked.

*Societal issues*

5. In this section of the paper, we examine wider societal consequences of the above developments. For the reasons already given, it is reasonable to expect that, *unless drastic measures of the sort proposed in Section 3 above are successfully implemented,* within the medium-term each individual in many societies will become associated with a large dataset of transferable longitudinal health data. This will happen *whether or not* that individual has given meaningful consent to its collection and processing. If this happens, what questions regarding the social implications of this development can we anticipate?

5.1 The first question concerns basic monitoring: will such data be accessible to the individual patient? To what extent and on what conditions? Will the patient have rights to establish how that data has been accumulated and whether its

accumulation accorded with the patient's consent, or happened without that consent? In so far as the answers to these questions are negative, the creation of such individual health datasets will represent a form of power *over* the individual patient exercised by the entities that control such data.

5.2 The second question concerns use: what restrictions, if any, will exist on which third parties can access such individual health data and on what terms? What entities will have access to it on a purely anonymous basis, and what entities will have unrestricted access? What restraints will exist to prevent anonymized data being open to de-anonymization once in the hands of third parties who are able to combine it with other datasets? What will the patient be able to discover about such uses of her data and the wider purposes which those uses serve? Will the patient be in a position to know when decisions affecting her have been made in reliance on such health data? Once again, in so far as the answers to these questions are negative, this will represent a form of power over the individual patient.

5.3 The third question concerns controls on use: what sorts of third-party usage of individual health data will be restricted and who or what entities will be able to enforce those restrictions? Will the costs of such enforcement be manageable by private individuals and, to the extent that they are beyond the ability of individuals to pay, what support will governments or other agencies provide to enable individuals to enforce their rights? To the extent that these questions do not receive satisfactory answers, this will represent a new form of inequality between individuals.

5.4 The fourth question concerns controls on government: what overriding rights will governments have in relation to accumulated health data, whether for reasons of law enforcement, welfare service management, crisis management, or general information gathering? Will governments seek preferential rights of access to such data as a matter of course, and what restrictions, if any, will exist to limit the application of such governmental rights of access? If unchecked, this represents a new dimension of governmental power over citizens.

5.5 If we assume that the answers to the above questions are uneven – that is, they help to reproduce a social landscape in which some individuals have more opportunities to protect their personal rights than others - then two further implications for society result: 1) first, such differences, driven as they are by deep

infrastructural forces in an important sector of the economy and society, are likely to become deeply embedded in social organization, resulting in permanent inequalities in how individuals and families are able, or not, both to protect their personal health data and protect themselves from decisions by powerful institutions based on that data; 2) second, the emergence and reproduction of such new inequalities will change how governments exercise their power, to the extent that governments will come to rely on the fact that some population groups are simply less able to protect themselves from data harm in relation to health data, one of the most personal forms of data. If so, how will governments, especially authoritarian governments, use that fact to further their own broader political projects?

5.6 In Section 7 we return to these questions and consider the likely outcomes if their trend goes unchecked.

*Public Health Emergencies: Lessons from COVID-19*

6. COVID-19 has provided an instructive glimpse into some of the issues discussed above as they concern public health, data collection, and the intersection of various public and private interests during a global health crisis.

6.1 Responses to the pandemic — which at the time of this writing is still unfolding, and whose impacts are still uncertain — have been informed by two assumptions that do not necessarily follow from each other: that the collection of data can help us understand and control the spread of the infection, and that this collection can be most efficiently carried out by surveillance technologies, often designed and deployed by private corporations in partnership with the state.

6.2 The debate over Bluetooth contact-tracing smartphone apps exemplifies the tensions that can arise in this context. The adoption of these apps, which can alert users if they come into contact with an infected person, is being encouraged with promises of effectiveness, respect for privacy, and a positive impact on personal safety and the common good. That these promises are sometimes being issued by corporations and governments with very poor track records in terms of defending individuals' privacy and the public good can perhaps only be explained by the confusion created by the pandemic. Nevertheless, important questions remain concerning the supposed effectiveness of these apps, since to date their reliability has not been empirically proved. Adoption without testing is a sure way

to institute invasive surveillance solutions without having to demonstrate their usefulness and necessity (already, half of those surveyed in the US are "skeptical that tracking someone's location through their cellphone would help curb the outbreak",[29] a significant figure given that this solution would require at least a 60% adoption rate to work). Furthermore, the characterization of these apps as easy and effective solutions obscures the fact that effective contact-tracing requires a much wider and intentional surveillance apparatus than individuals' phones can provide. In South Korea, for example, authorities conducting contact-tracing can assemble a citizen's profile that includes GPS phone data, credit-card payment information, travel history and medical records in under a minute (given that Seoul is twice as dense as New York City, Bluetooth contact tracing alone would not be sufficiently effective).[30]

6.3 It is important to note that resistance to the introduction of health data surveillance solutions such as contact-tracing apps is already present. Groups within civil society — including activists, scientists, academics and tech workers — have raised an alarm against the suspension of civil and human rights under the pretence of an emergency response, especially in light of states' recent track record of extending such responses beyond times of crisis (as happened in the aftermath of terrorist attacks at the beginning of the century). But the imposition and acceptance of such emergency measures also varies according to geopolitics, and depends on how each society makes sense of encroachments into personal privacy. In societies that consecrate the rights of the individual, at least at the level of rhetoric, the imposition of emergency health data surveillance might be seen as acceptable if it is accompanied by narratives of technological innovation and progress, trust in corporations and their products, safety from threats, and personal choice (in these cases, a decentralized system for the collection of data, where data is not available for analysis by one distinct authority, seems to be favoured, although its effectiveness has not yet been proven). In societies where the interests of the individual are seen as subordinate to the public good, the state is acknowledged as having absolute power to impose emergency measures build on already established systems of surveillance, something it can do in close collaboration with corporations (as in the case of China).

6.4 While well-intentioned, health data surveillance solutions such as the Bluetooth tracing apps can generate social graphs (information about who is socially related

to whom) that can be abused to spy on citizens' activities if both the storage and use of such information is not adequately controlled.[31] But privacy concerns are not the only factors to consider when determining the value and effectiveness of emergency solutions that rely on the collection of data that, in the context of a public health crisis, is deemed relevant to health. Since these solutions can be appropriated by legitimate or illegitimate actors (including oppressive regimes, exploitative businesses, and criminal hackers), they can have direct effects on individuals' freedom of association and movement, the right to safety and health care, and the right to non-discrimination.[32]

6.5 The question of the development of emergency technological systems also brings to light complicated issues of technology transfer between the Global North and South. SORMAS (the Surveillance, Outbreak Response Management and Analysis System; https://sormasorg.helmholtz-hzi.de/) illustrates the opportunities as well as the limits of such collaborations. SORMAS was developed to provide real-time digitalized reporting and response management to enable outbreak containment. The platform, developed primarily with expertise and resources from the German Federal Ministry of Education and Research, the Centre for Infection Research, and the Corporation for International Cooperation, was successfully deployed during the West Africa Ebola outbreak of 2014-15 and continues to expand to other locations and situations. The system is built with open-source technologies and takes into consideration connectivity and usability issues from a Global South perspective; the interface and process workflows were designed with input from the users themselves. However, when it comes to data privacy issues, the German developers seem to avoid responsibility and adopt a view of their technology as neutral by stating that data generated in SORMAS "belongs to the national authority in charge and is stored according to national requirements."[33] In some cases, this might not afford citizens the privacy they are entitled to, and might leave the door open for abuse and targeting of vulnerable groups by governments.

*Looking to the Future*

7.1 We already considered in Section 5 the broader social harms which may flow from failure to attend to the issues identified in Section 3 from the unrestrained growth of personal and collective health data, a trend which commercial incentives are very likely to accelerate (Section 4). In this section, we ask what sorts fo societies

will result if such directions of change are not urgently interrupted: in other words, what are the *social futures* for today's younger generations that are likely to result from a failure to address the issues concerning personal health data that are already prominent?

7.2 Our prediction is that, without very strong and urgent policy interventions in the next 2-3 years (interventions to which the Commission may well contribute), the following trends will stabilize: (1) the normalization of personal health data collection across contemporary societies without effective mechanisms for most individuals to opt out (opting out will become increasingly expensive, while the 'convenience' of opting in will increasingly be taken for granted); (2) the lack of availability for all but the wealthy and educationally empowered to contest such abuses of their personal health data as they arise; (3) the integration of uses of personal health data into decision-making in an increasing range of sectors of importance to individuals' and families' well-being (from finance to insurance to health services to workplace management to social security); (4) the increasing sense that individuals are responsible for the good management of their personal health data without having the resources to challenge or control how such data is collected and used, and on what terms, and with what authority; (5) the increasing sense that governments see the good management of both public health and welfare services as depending on their management of such health data, and so they will become less, not more, likely to intervene to limit the growth and circulation of personal health data. In addition (6) governments in all but the richest countries will become increasingly dependent on larger players in the health data sector (such as Google), and so become less, not more, likely to regulate effectively the protection of privacy in relation to the growth and circulation of personal health data; and finally (7), as the rhetoric of 'dataism' grows in most societies,[34] good health policy will increasingly be associated with the optional production and circulation of health data without sufficient attention to the social externalities and risks associated with such data production.

7.3 Under the future circumstances sketched in 7.2, we predict that far from the protection of privacy of personal health data being a stable principle, it will increasingly become a background option that is, by default, *switched off* for all but the most empowered individuals. The results will not necessarily be bad for individuals, because the benefits from increasing health data flows may contribute

to possibilities for more effective treatment. But the likelihood will be that, for populations that are already disadvantaged and vulnerable to harsh treatment, their lack of control over the management and use of their personal health data will become a further strand in what US scholar Mary Madden calls the 'matrix of vulnerabilities' affecting disadvantaged populations in a datafied society.[35]

7.4 In so far as vulnerabilities to harms in relation to personal health data affect individuals, they affect particularly badly those groups that are already exposed to health risks and/or data harms (section 1.4 above).

7.5 None of the above predictable trends will be averted, in our judgement, unless strong and urgent action is taken now to change the direction of travel in relation to personal health data and to limit more effectively the unrestrained collection and processing of such data.

*Conclusion*

8. The argument of this submission to the Commission on Governing Health Futures can be summarized as follows:

8.1 Large commercial forces are driving the expanded collection, generation and aggregation of health and health-related data for the extraction of economic value. The protection of individual privacy rights in relation to such data is not a primary motive of those commercial forces. There is no reason to trust that markets left to themselves will generate sufficient protections of individual rights in relation to health data. A global debate about legislative and regulatory intervention is needed, and that debate must have recourse to the language of human rights. From that basis, the beginnings of an agenda for legislative and regulatory intervention can be forged and this paper has made some tentative proposals for consideration (section 3).

8.2 At this point in history however, global policy debate on big data and artificial intelligence has been overwhelmingly shaped by commercial discourse on AI and big data, which tends to prioritize the maximization of data production and unrestricted data flows.[36] The OECD's AI principles mention human rights in passing, but make no reference to the possibility that data collection and transfer might need to eb restricted in order to protect such rights.[37] The United Nations Development Programme (UNDP) in its pronouncements on AI and big data, including in the area of health, rather than alerting global debate to issues

concerning privacy, has instead repeated the principle that “Ultimately, AI is not good or bad in and of itself. It’s all about how we choose to use it”,[38] a statement which ignores completely any issues about the collection and construction of data.[39] Privacy considerations have until now been secondary in such international NGO discourse, relying implicitly on the claim that data are “just there”, ready to be used, provided that they are used well. But health data, like all data, is not raw material, but rather the product of a complex industrial and technological infrastructure for the *construction* of data from the flow of our bodies’ lives. Health data are not “just there”, and only come into being under particular social conditions, which can be challenged and contested, and indeed must be if processes of datafication are to conform more closely to the principles of protecting human rights.

8.3 Public health crises, such as COVID-19, can be problematic times to introduce health data surveillance measures. While there might be a real need to collect and analyse health data through emergency interventions, the perceived need and benefit must be balanced with actual testing of proposed solutions’ usefulness, a careful assessment of the impact of the surveillance actions on privacy and other human and civil rights, a commitment to transparency and openness, and time-limit considerations that specify when the collection of data will stop. Unfortunately, times of crisis are not conducive to this kind of careful assessment, which means society must remain particularly vigilant.

8.4 Leaving to one side the Covid-19 crisis, contemporary societies face a crossroads: *either* take seriously the already noted risks of enhanced inequality stemming from failure to address health data harms, *or* guarantee that inadequate protection of personal health data is normalized as one of the matrix of vulnerabilities associated with long-term inequality in future societies. Taking the first path requires the urgent rethinking of how health data issues are addressed and managed, paying close attention to the social externalities we have identified and their implications for whole societies and not just individuals. Such rethinking needs to emerge from inclusive deliberations, that is, a society-wide discussion that learns from representatives of groups that are likely to be most disadvantaged from the massive growth of health data.

8.5 We submit that an important role of the Commission on Governing Health Futures, both in times of crisis and normalcy, is to challenge the conditions under which

health data is produced and circulated, arguing for such processes to be governed in accord with the right of each human being to have control over the flow of information about her life, including that life's most basic dimension: health. To do so, the Commission must encourage the widest possible social conversation about the generation and management of personal and population-wide health data, a conversation that moves beyond narrow definitions of individual data harms and individual data rights, from which those who are already advantaged are most likely to benefit. If, as we have argued, the protection of personal health data is essential to the integrity of each person's life, organizing societies around poor or uneven protection of personal health data means organising societies around the *assumption* that the integrity of many individuals and groups will be compromised. That is not a responsible direction for any society to take. The challenge therefore for the Governing Health Futures Commission is to encourage that more inclusive conversation about health data to start now.

**NICK COULDRY, PROFESSOR OF MEDIA COMMUNICATIONS AND SOCIAL THEORY, LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE.**

**ULISES A. MEJIAS, ASSOCIATE PROFESSOR OF COMMUNICATION STUDIES, STATE UNIVERSITY OF NEW YORK, OSWEGO.**

**Revised JULY 2020**

---

[1] See the Hippocratic Oath: https://www.pbs.org/wgbh/nova/doctors/oath_classical.html
[2] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E
[3] For discussion, see Rouvroy, Antoinette, and Yves Poullet. (2009) "The Right to Informational Self-determination and the Value of Self-development." In *Reinventing Data Protection?,* edited by Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne, and Sjaak Nouwt, 45–76. New York: Springer.
[4] Citing Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union. Article 8(1) states that "everyone has the right to respect for his private and family life, his home and his correspondence", a principle also reflected in The Fourth Amendment to the US Constitution.
[5] GDPR Recital 35.
[6] GDPR Recital 54, compare Article 9(2)(i).
[7] GDPR Recital 53.
[8] Barbara J. Evans "Barbarians at The Gate: Consumer-Driven Health Data Commons and The Transformation of Citizen Science." *American Journal of Law & Medicine* 42, no. 4 (2016): 651-685.
[9] Evans op. cit.
[10] https://undocs.org/A/74/493
[11] Virginia Eubanks (2018) *Automating Inequality*. New York, NY: St. Martin's Press.
[12] Shoshana Zuboff (2019) *The Age of Surveillance Capitalism*, London: Profile Books, 247-251.

[13] Nick Couldry and Ulises A. Mejias (2019) *The Costs of Connection*. Stanford: Stanford University Press.
[14] Daniel Sulmasy, "Naked Bodies, Naked Genomes: The Special (But Not Exceptional) Nature of Genomic Information." *Genetics in Medicine* (2014). DOI: 10.1038/gim.2014.11.
[15] GDPR Recital 53
[16] Ruth R. Faden, Nancy E. Kass, Steven N. Goodman, Peter Pronovost, Sean Tunis, and Tom L. Beauchamp. "An Ethics Framework for a Learning Health Care System: A Departure from Traditional Research Ethics and Clinical Ethics." *Ethical Oversight of Learning Health Care Systems, Hastings Center Report Special Report* 43, no. 1 (2013): S16–2, at S23.
[17] Evans, op. cit. 5; Bonnie Kaplan, "Selling Health Data: De-Identification, Privacy, and Speech." *Cambridge Quarterly of Healthcare Ethics* 24, no. 3 (2014): 256–71, at 261; Timothy Caulfiel, Sarah Burningham, Yann Joly, Zubin Master, Mahsa Shabani, Pascal Borry, Allan Becker, et al. "A Review of the Key Issues Associated with the Commercialization of Biobanks." *Journal of Law and the Biosciences* 1, no. 1 (2014): 94–110, at 108.
[18] GDPR Recital 26.
[19] Latanya Sweeney, "Health Data Flows." Seminar at Federal Trade Commission, Washington, DC, May 7, 2014. https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf
[20] Elettra Bietti (2019) "Consent as a Free Pass: Platform Power and the limits of the Informational Turn", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3489577
[21] Nathan Heller, "Estonia, the Digital Republic," *The New Yorker* (December 18 & 25, 2017).
[22] European Commission (2020) "A European Strategy for data", https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf at 2, 22, 29-30.
[23] European Commission (2020) "On Artificial Intelligence: A European approach to excellence and trust", https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, at p. 8.
[24] Elettra Bietti, Nick Couldry, Gretchen Greene, and Velislava Hillman (2020) Response to the European Commission White Paper on AI, COM 2020-65, April: https://medium.com/berkman-klein-center/response-to-the-european-commissions-white-paper-on-artificial-intelligence-a525432b6dec .
[25] See for example in the USA https://www.federalregister.gov/documents/2020/01/13/2020-00261/request-for-comments-on-a-draft-memorandum-to-the-heads-of-executive-departments-and-agencies
[26] Rob Copeland and Sarah Needleman, (2019) "Google's 'Project Nightingale' Triggers Federal Inquiry', *Wall Street Journal,* 12 November.
[27] Sarah Needleman and Rob Copeland, (2019) "Google Counts on Fitbit to Make Imprint in Health Market", *Wall Street Journal,* 6 November.
[28] James Rundle and Angus Loten, (2019) "The Power of Combining 5G with AI", *Wall Street Journal,* 8 November.
[29] Pew Research (2020) "Most Americans don't think cellphone tracking will help limit COVID-19, are divided on whether it's acceptable". https://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable
[30] Kim, Max S. (April 17, 2020). Seoul's Radical Experiment in Digital Contact Tracing. The New Yorker. https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing
[31] Joint Statement on Contact Tracing. April 19, 2020. https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view
[32] Letter to Ministry of General Affairs by Dutch academics "Re: COVID-19 tracking- and tracingapp and healthapp." Amsterdam, April 13,2020. http://allai.nl/wp-content/uploads/2020/04/Online-version-Letter-to-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-re.-COVID-19-apps.pdf
[33] See the product brochure at http://danieltomaba.com/sormas/SORMASFlyerTablet.pdf
[34] Jose van Dijck (2014) (2014) "Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology." *Surveillance & Society* 12, no. 2: 197-208; Yuval Harari, (2015) *Homo Deus*. London: Vintage Books.
[35] Mary Madden, Michelle Gilman, Karen Levy, and Alice Marwick (2017) 'Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans.' *Washington University Law Review,* 95: 53-125.
[36] Nick Couldry and Jun Yu, (2018) 'Deconstructing Datafication's Brave New World', *New Media & Society* 20(2): 4473-4491.

[37] https://www.oecd.org/going-digital/ai/principles/
[38] https://www.undp.org/content/undp/en/home/blog/2018/ai-and-the-future-of-our-work.html
[39] Couldry and Yu, op cit, 4477-4478.