

Health data and global power inequalities: challenging the world data order

Dados sobre saúde e desigualdades de poder globais: desafiando a ordem global sobre dados

Datos de salud y desigualdades de poder global: desafiando el orden mundial de datos

Nick Couldry^{1,a}

n.couldry@lse.ac.uk | <https://orcid.org/0000-0001-8233-3287>

Ulises Ali Mejías^{2,b}

ulises.mejias@oswego.edu | <https://orcid.org/0000-0003-3774-0195>

¹ London School of Economics and Political Science, Department of Media and Communications. London, United Kingdom.

² State University of New York, School of Communication, Media and the Arts. Oswego, NY, United States.

^a Ph.D in Media and Communications by the University of London.

^b Ed.D in Technology and Communication by Columbia University.

ABSTRACT

Today's global media infrastructures involve not just media, but the continual extraction and circulation of data across digital platforms, with health data being an important data domain. The extraction and use of health data raises particular human rights issues. This paper reviews, first, the basic risks to individuals from unconstrained collection, use and transfer of their personal health data; second, the implications of the fast-growing health data sector for social power generally; and third, the wider implications if current trends related to commercial exploitation of personal health data are not interrupted. A new global debate is needed to address these trends and their basis in a highly unequal political economy which benefits the same countries that profited from historical colonialism. We articulate here — in new ways — the challenges addressed by the 1980 MacBride Report, but for a very differently configured world.

Keywords: Health data; Health-related data; Social externalities; Power; Human rights.

RESUMO

As infraestruturas de mídia de hoje envolvem não apenas mídias, mas também a contínua extração e circulação de dados através de plataformas digitais, com dados sobre saúde constituindo um importante domínio de dados. A extração e uso de dados sobre saúde gera questões especiais sobre direitos humanos. Este artigo avalia, primeiramente, os riscos básicos para indivíduos com a coleta, uso e transferência irrestritos de seus dados pessoais de saúde; em segundo lugar, as implicações para estruturas sociais de poder em geral do setor de dados de saúde, que vem crescendo rapidamente; e em terceiro lugar, as implicações gerais caso as tendências atuais relacionadas à exploração comercial de dados pessoais de saúde não sejam interrompidas. Um novo debate global é necessário para fazer face a essas tendências e sua base em uma economia política altamente desigual que beneficia os mesmos países que se beneficiaram historicamente do colonialismo. Nós expressamos aqui — de forma original — os desafios abordados no Relatório MacBride de 1980, mas para um mundo com uma configuração muito diferente.

Palavras-chave: Dados sobre saúde; Dados relacionados à saúde; Externalidades sociais; Poder; Direitos humanos.

RESUMEN

Las infraestructuras de medios globales de hoy en día involucran no solo a los medios sino también a la extracción y circulación continua de datos a través de plataformas digitales y los datos de salud son un dominio de datos importante. La extracción y el uso de datos de salud coloca problemas particulares de derechos humanos. Este artículo revisa, en primer lugar, los riesgos básicos de las personas con la recopilación, el uso y la transferencia sin restricciones de sus datos personales de salud; en segundo lugar, las implicaciones del sector de datos de salud en rápido crecimiento para el poder social en general; y tercero, las implicaciones más amplias si no se interrumpen las tendencias actuales relacionadas con la explotación comercial de datos personales de salud. Es necesario un nuevo debate global para abordar estas tendencias y sus bases en una economía política altamente desigual que beneficia a los mismos países que se beneficiaron del colonialismo histórico. Aquí, articulamos – de nuevas maneras – los desafíos abordados por el Informe MacBride de 1980, pero para un mundo configurado de manera muy diferente.

Palabras clave: Datos de salud; Datos relacionados con la salud; Externalidades sociales; Poder; Derechos humanos.

INFORMAÇÕES DO ARTIGO

Contribuição dos autores:

Concepção e desenho do estudo: Nick Couldry, Ulises Ali Mejías.

Aquisição, análise ou interpretação dos dados: Nick Couldry, Ulises Ali Mejías.

Redação do manuscrito: Nick Couldry, Ulises Ali Mejías.

Revisão crítica do conteúdo intelectual: Nick Couldry, Ulises Ali Mejías.

Declaração de conflito de interesses: none.

Fontes de financiamento: none.

Considerações éticas: none.

Agradecimentos/Contribuições adicionais: Thanks to Professor Ilona Kickbusch, Graduate Institute for International and Development Studies, Geneva, Switzerland, for inviting the research which led to this article.

Histórico do artigo: submetido: 29 out. 2020 | aceito: 29 out. 2020 | publicado: 17 dez. 2020.

Apresentação anterior: none.

Licença CC BY-NC atribuição não comercial. Com essa licença é permitido acessar, baixar (*download*), copiar, imprimir, compartilhar, reutilizar e distribuir os artigos, desde que para uso não comercial e com a citação da fonte, conferindo os devidos créditos de autoria e menção à Reciis. Nesses casos, nenhuma permissão é necessária por parte dos autores ou dos editores.

Forty years ago, Unesco published the MacBride Report (Many Voices, One World), which called for a New World Information and Communication Order to challenge the West’s dominance over the global media infrastructures of television, radio, the press and film. Today, faced with radically transformed media infrastructures, the world once more needs alternatives to the trajectories already mapped out by Big Tech companies in North America and China. Our era’s urgent questions relate not so much to the export of programme formats and the training of journalists, but rather to the regulation of digital social platforms and internet search engines and, more acutely, the massive opportunities for personal data extraction that come with ownership of those platforms. Whereas it would have made no sense to involve the health sector in calls for more just media infrastructures 40 years ago, today it absolutely does, because health data is, as the Wall Street Journal recently put it, an “open frontier”¹ for data extraction by corporations such as Apple, Googleⁱ, and many others. In this short paper we review the implications of today’s media infrastructures with respect to health data and – more broadly – for human freedom. There is, as we shall see, no time to be lost in initiating this debate.

Health is a fundamental dimension of life: an individual’s health is the matrix of factors which determines whether his or her life continues. Health data are therefore among the most personally significant data about a person. Every sphere 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 is no exception.

Data about a person’s health are highly significant to that person’s life. Each individual’s right to control the information produced and circulated about their health is therefore a fundamental aspect of their personal integrity. Health data affects human rights: indeed, as UN Human Rights Commissioner Michele Bachelet has stated, the “digital revolution” (of which datafication ‘on an industrial scale’ is unmistakably a part) “is a major global human rights issue”².

No one doubts that the science of health (medicine) requires the production, aggregation and analysis of health data. The more contextually rich these data are, the more scientifically useful they 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’ (for example, via devices such as the Fitbit or Apple Watch). The potential benefits for medical knowledge are huge, but the potential societal risks of datafication in the health sector are also immense. As a result, contemporary societies face a problem: how to balance 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 recent growth of the health data sector, within and beyond the medical profession, is creating broader economic and social pressures for a general market in health data. It is particularly important to identify the ‘social externalities’ that will result when flows of personal health data are encouraged beyond the two types of restricted circumstances under which personal health data has until now been expected to flow: within the scope of the confidential doctor-patient relationship and for exceptional public health emergency reasons.

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 others from the specific health risk which that individual represents, and it means quite another thing to an insurer concerned with limiting the business costs of a policy by identifying exclusions to it. Insurers are only the most obvious example of ‘non-medical actors’ that have an interest

i In November 2019, Google acquired Fitbit for US \$2.1 billion.

in getting access to personal health information. Providers of personal finance products 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. Government welfare payment agencies will likewise be interested in accessing personal health data. Marketers, in a more indirect way, may be able to benefit from health data available along with 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, leads to the risk of unequal power relations in society.

One approach, in response, is to consider the broader transformation in global economies under way in this context. Management theorist Shoshana Zuboff argues that these general trends exemplify 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"³. More broadly, this trend can be seen as part of a new colonial stage of capitalism (what we call 'data colonialism') in which, echoing the historic colonial land grab of resources that made capitalism possible, human life itself is becoming the new target of economic extraction⁴. Exploring those debates would take up more space than we have here.

Let us focus instead on the specific social externalities of health data flows.

BASIC RISKS

Even in situations in which 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. Health data storage will come to depend, if it does not already, on cloud computing, that is, shared servers belonging to corporations from which medical practitioners lease storage rights. Clear rules are needed to ensure that this data storage remains under the control of medical professionals and complies with applicable confidentiality obligations. However, some health data are so sensitive to the individual in question that their storage should be allowed only under special conditions, for example the data that describes someone's genome.

Leaving aside the exceptional case of the human genome, health data is normally dealt with in standard ways. 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 reliable⁵. But this second assumption is not true: as a number of US medical legal scholars point out, anonymized health data can, 'when combined with other data', yield the identity of the person⁶⁻⁸. 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 of health and health-related data to data controllers (whether single actors or distributed networks) and aggregation by them be imposed'. Serious consideration is therefore needed to restrict the exchange of health data unless and until the risks of de-anonymization can be mitigated.

A specific version of the general risk of de-anonymization arises when anonymous health data is transferred between contexts (*e.g.* from a patient-doctor relationship to a general therapeutic relationship, or to another context such as self-improvement, employment, or commercial services). The progressive risk of de-anonymization accumulates as data is transferred between more and more contexts. Nevertheless, the 'seamless' flow of health data, as with other data, is often proposed as a business ideal. On the contrary, we argue that seamless data flow should 'never' be proposed as a norm in the health sector without first ensuring that secure protections against the potential problems related to de-anonymization are in place.

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.

To address such risks, more robust rules are needed, such as: (1) rules to enforce transparency regarding any transfer of health or health-related data to a third party beyond that strictly necessary for the functioning of a device; (2) restrictions on powerful actors to prevent them from requiring or strongly incentivising adoption by others (for example, employees) of a health self-tracking device, as this would effectively impose that device's data collection terms and conditions on its users; and (3) severe restrictions on the gathering of locational and other social data by self-tracking devices and apps whose purported purpose is health enhancement.

AN EXPANDING HEALTH DATA SECTOR

We just examined the basic risks to human rights from the collection and processing of health and health-related data. We also proposed legal rules to limit those risks. These rules may or may not be successfully implemented by various legislatures. Even if they are, the result may not be sufficient to halt the very powerful commercial forces currently driving the expansion of the health data sector. What might be the implications if that sector continues to grow unconstrained?

While this requires much more space than we have here, we can summarise the situation by saying that there is clear evidence of major commercial pressures for the expansion of artificial intelligence (AI) in the health sector, with all the pressures to collect and circulate 'personal' health data that inevitably arise from this. Google is a leading global player in AI and its attempts to obtain data from health authorities have attracted attention, such as in the United States and the UK. Apple is also another key player.

Without going into detail, it is reasonable from this to anticipate that new health data infrastructures will emerge, bound together by alliances between the large players in the health sector (physicians' networks, regional health provision systems, device providers, Big Tech providers of cloud services and AI analytics, and health insurers). The establishment of these infrastructures — first of all, in the most economically developed countries (such as the United States), 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 these trends or get access to effective alternatives. Insofar as privacy-protection options are available within this transformed health infrastructures, 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 to effectively compel policyholders to accept existing data processing terms.

WIDER SOCIAL CONSEQUENCES

The first question concerns basic monitoring: will the individual patient have access to this data? To what extent and under what conditions? Will the patient have the right to establish how that data has been gathered and whether or not its collection was in accordance with the patient's consent?

The second question concerns use: what restrictions, if any, will exist regarding which third parties can access individual health data and on what terms? Which entities will have access to it on a purely anonymous basis, and which will have unrestricted access? What restraints will exist to prevent anonymized data from being subject 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 that those uses serve?

A third question concerns controls on use: what sorts of third-party usage of individual health data will be restricted and who or which 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?

A 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, and what restrictions, if any, will exist to limit the application of such governmental rights of access?

Unless the above questions receive satisfactory answers, there will be major implications for the redistribution of power over health data, a redistribution that benefits corporations and, to some degree, governments – not private individuals.

Two further implications follow. First, these differences, driven as they are by deep infrastructural forces in an important sector of the economy and of society, are likely to become deeply embedded in social organization, resulting in permanent inequalities in the degree to which individuals and families are able to protect their personal health data and protect themselves from decisions by powerful institutions based on that data. Second, the emergence and reproduction of these 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?

CONCLUSION

We have laid out these issues without specific reference to the political economy of any particular nation. It should be obvious however that the nations that are best placed to resist these trends are those which either host Big Tech companies or which have strong economies and regulatory systems – in both cases, for reasons linked inextricably to the distribution of power during historic colonialism. The nations which are worst placed to resist these pressures are those which have historically suffered from the consequences of colonialism. In this way, data colonialism risks strengthening still further the grip of colonial power on the world's resources. The need for a profound reassessment of today's global media infrastructures in all respects, but particularly health information, is thus sadly confirmed.

REFERENCES

1. Needleman S, Copeland R. Google counts on fitbit to make imprint in health market. Wall Street Journal [Internet]. 2019 Nov 06 [cited 2020 Nov 17];Tech. Available from: <https://www.wsj.com/articles/google-counts-on-fitbit-to-make-imprint-in-health-market-11573052061>.
2. Human rights in the digital age: can they make a difference? Office of the High Commissioner for Human Rights [Internet]. 2019 Oct 17 [cited 2020 Nov 17];News and Events:DisplayNews. Keynote speech by Michelle Bachelet, UN High Commissioner for Human Rights Japan Society, New York. Available from: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E>.
3. Zuboff S. The age of surveillance capitalism. London: Profile Books; 2019.
4. Couldry N, Mejias UA. The costs of connection. Stanford: Stanford University Press; 2019.

5. Faden RR, Kass NE, Goodman SN, Pronovost P, Tunis S, Beauchamp TL. An ethics framework for a learning health care system: a departure from traditional research ethics and clinical ethics. *Hastings Cent Rep.* 2013 Jan-Feb;Spec n:S16-27. doi: <https://doi.org/10.1002/hast.134>.
6. Evans BJ. Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science. *Am J Law Med.* 2016 Nov;42(4):651-685. doi: <https://dx.doi.org/10.1177%2F0098858817700245>.
7. Kaplan B. Selling health data: de-identification, privacy, and speech. *Camb Q Healthc Ethics.* 2015 Jul;24(3):256-71. doi: <https://doi.org/10.1017/s0963180114000589>.
8. Caulfield T, Burningham S, Joly Y. et al. A review of the key issues associated with the commercialization of biobanks. *J Law Biosci.* 2014 Feb 25;1(1):94-110. doi: <https://dx.doi.org/10.1093%2Fjlb%2F1st004>.