Why paying individual people for their health data is a bad idea

Paying individual people for their health data will widen inequalities and reduce altruism, luring people to sell their privacy. Health data should instead be treated as collective property, and commercial profits should be shared with the public.

Barbara Prainsack and Nikolaus Forgó

Data use in the digital age is fundamentally different from that in the paper age, with ever more aspects of our bodies and lives being recorded in digital data[1]. There is also an increasing power asymmetry between citizens and the organizations that use their data. Public bodies and companies hold so much data and information about people that this relationship has been called a one-way mirror[2]. Some of the benefits and harms emerging from data use affect specific individuals or groups of people. But other benefits and harms are systemic, and felt not only by the person from whom the data come but also by a much wider range of people, or even by society as a whole.

Some commercial companies and data rights activists have proposed that citizens should be paid for their data. The idea is simple: whenever a company uses personal data, they should pay the individuals contributing the data. One mechanism for this is a royalty model, in which people get paid whenever their data are used, even if it is reused by the same company. As artificial intelligence (AI) needs ever more data, licensing data to AI companies, it has been argued, could become a new source of income[3].

At first sight, paying people for their health data may seem compelling. Everyone generates data in their roles as patients, shoppers, and users of digital services and devices. Although data are often called the new oil[4], data, unlike oil, are created by people — so why should people not be rewarded for its use?

Table 1 | Harms caused by paying people for their health data

Harm	Effect
Dependence	People become dependent on the income from selling their data, so they cannot easily protect or regain their privacy
Exacerbation of inequalities	Those on low incomes sell their privacy, while those on high incomes do not need to, exacerbating inequalities in and between societies
Reduced accuracy	Some data may pay better than others, which may lead to biases or falsified data
Reduced altruism	If people expect to be paid for their data, some will no longer allow free data access to nonprofits or health systems, who rely on these data to improve patient health

Increasing inequalities

Paying people for data is problematic, as it would allow the rich to pay for services with money, while people on low incomes pay with data and concomitant loss of privacy[5]. For example, under a pay-for-use regime, a medical imaging company developing software that detects skin cancer would need to pay each patient whose data they use in the process. The licence agreement might state that the company may share the data with third parties for the purpose of marketing, and some people might sign this, despite misgivings, because they needed the money. Moreover, people in low-income countries are likely to get significantly less remuneration than those in high-income countries if the fee is adjusted to the local living standards and the achievable market price.

Harms at several levels emerge in this scenario (Table 1). Some people who get paid for their data will become locked into this arrangement by their dependence on this income. Even if the company uses their data for purposes that they do not support, or if they are concerned about possible discrimination, they will have to agree to the terms in order to continue receiving an important source of income.

Paying individuals for their data would exacerbate global inequities and increase the level of surveillance to which people on low incomes are exposed. The poorest people in the world, sometimes referred to as 'bottom-of-pyramid consumers', have already been targeted by companies who know that they are more willing than others to trade personal information for discounts or benefits. Phone companies have offered airtime or mobile data in return for access to the data stored on people's phones or to their telephone logs, or in return for filling out surveys[6,7].

Paying people for their data also may lead to distortions in the data itself, as it may create an incentive to create the data that pay the most. For example, if data about a specific disease pays particularly well, this might lead to changes in behaviour, data falsification and over-reporting of the disease.

Paying people for their data will also reduce altruism. If people expect to get paid for the use of their data, they are unlikely to give it away for free. This provides an advantage to wealthy corporations compared to smaller enterprises or nonprofit organisations. Some research for the public benefit may no longer take place, because the public hospitals or charities that were previously carrying out the research cannot afford to pay for the data.

Some of this is already happening. Starting in 2015, Amgen offered patients a cholesterol-reducing drug for a significantly discounted price if they allowed the company to access and use their personal data[8]. Other companies, inside and outside the health sector, offer similar deals or benefits in return for data[9–11].

Collective property

There is no clear agreement about who owns personal data. Ownership is not the same as

Table 2 | Differences between property and ownership

Property	Ownership
An individual right that has to be assigned to someone with legal personality	An individual or collective right, which is not necessarily assigned to someone with legal personality
Law in rem (legal action is taken against the holder of a thing, not against a person as such)	Not necessarily a law in rem
Relatively stable concept, stemming from Roman legal traditions and fully reflected in contemporary law	Flexible concept, incorporating modern ideas of information law and not fully reflected in contemporary law

Table 3 | Decision levels on ownership

Level	Decision mode
Commons and communities	Joint decision-making by everyone who contributed data, either directly or via a delegation
States	Public deliberation, such as by citizen juries, patient or data user advisory boards, or national legislation
Supranational or international organizations	EU law and international treaties

property: it can also refer to a moral claim on something. People who say that they own their personal data often mean that they want to have a say in who uses them, what they do with them and who benefits from this, and to prevent their data from being used against them. It is a statement about control over data, and ultimately about dignity and autonomy.

At other times, ownership is used to refer to property rights (Table 2). Property rights are a bundle of entitlements that grant control to the rights holder. This includes the right to do whatever they want with the object and to exclude everyone else from doing the same; these two entitlements set property rights apart from other kinds of ownership, such as usage rights[12]. Debates on property rights to data typically assume that these rights are, or should be, held by individual citizens or organisations.

Instead of endorsing individual-level property rights to data, we should consider health data as collective property[13]. Although individuals should have direct control over their data wherever this helps to protect their privacy and dignity (including individual consent to data use in the context of medicine or insurance), data property rights should be a collective, not an individual, right. Communities and nations should decide how data should be used and for whose benefits[14] (Table 3). In contrast to open-access regimes, in which data can be taken by anyone and is often used most profitably by those with the deepest pockets, collective property rights would enable communities to exclude certain types of user, such as large technology companies, or impose conditions of use.

Better legislation

Several data misuses have led to public outrage in recent years, including transfers of patient data to private companies without people's knowledge, as well as accidental data leaks. These have decreased public trust in the safety of personal data in the healthcare system and increased discontent about the seemingly unlimited power of technology companies and other multinational corporations.

Data misuses can be tackled with more effective legislation. Practices that harm individuals or communities, such as the unwanted transfer of sensitive personal data to a social media service[15] or delays in releasing information on data breaches[16], should be outlawed, with fines high enough and enforcement mechanisms effective enough to deter powerful commercial players, who often have deep pockets, from breaking the law. Moreover, governments must end their 'comfortable friendship with the digital giants'[17]. Many tech companies have so much influence on policy that they have become quasi-regulators[18]. Rather than limiting the power of tech giants, governments have enabled their power to grow and allowed them to enter new markets, such as the healthcare market.

Fairer taxation

Many companies have entered the health sector using a 'free data for free service' model. These companies have an advantage over other businesses in that there is currently a de facto exemption from taxation for services that people buy with data instead of money. When people get access to seemingly free services in exchange for their personal data, these transactions are not taxed. If people pay for these same services with money, the same transactions are taxed[19]. For example, if a person looks for dietary advice, while taking a specific drug, via an online search engine, the owner of the search engine can analyze and profit from this user's data, with no tax due. If the same person paid a dietician to give them the same advice, the dietician would need to pay tax on this income.

There is a global justice dimension to taxation, as many businesses in the digital health economy have a significant economic presence in the Global South, yet have no obligation to pay taxes in these countries because they are headquartered elsewhere[20]. Taxes on digital health businesses could help to offset such global inequities. Ideally, such taxes would be proportional to the volume of patient data used and would consider the extent to which the activity creates public value. Businesses using more data, and those that create little or no public value could pay more tax, although assessing data volume and public value is extremely difficult. A more realistic solution may be a general corporate tax for digital businesses.

Buying privacy

Paying individual people for their data may superficially appear emancipatory, but it is highly problematic. Individual-level monetization is likely to lead to a situation in which the rich pay with money, whereas people on low incomes pay with data. The negative effects from this will be especially felt in societies where there is limited public healthcare and a reliance on the private purchase of health and other services, leading to an increase in social and economic inequalities, so that privacy becomes a privilege of the wealthy.

A more equitable solution is for data to be treated as collective property that is jointly owned and governed by citizens. If combined with the prohibition of harmful data practices and corporate taxation mechanisms fit for digital economies, these measures will help to ensure that people and communities benefit from the use of their health data. ❐

Barbara Prainsack ✉ and Nikolaus Forgó
Research Platform Governance of Digital Practices, University of Vienna, Vienna, Austria.
✉*e-mail: barbara.prainsack@univie.ac.at*

Published online: 12 September 2022
https://doi.org/10.1038/s41591-022-01955-4

References

1. Kickbusch, I. et al. *Lancet* **398**, 1727–1776 (2021).
2. Wellcome Trust and Ipsos MORI Social Research Institute. https://www.ipsos.com/sites/default/files/publication/5200-03/sri-wellcome-trust-commercial-access-to-health-data.pdf (2016).
3. Aiello, C. *CNBC* https://www.cnbc.com/2018/06/21/tech-pioneer-jaron-lanier-says-companies-should-pay-for-data.html (2018).
4. *The Economist* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (2017).
5. Elvy, S. A. *Colum. L. Rev.* **117**, 1369 (2017).
6. AfriSight. Panelist Portal https://afrisight.com/en (2022).
7. Tarran, B. *ResearchLive* https://www.research-live.com/article/opinion/janas-eagle-one-of-50-people-who-will-change-the-world/id/4006814 (2012).
8. Hiltzik, M. *Los Angeles Times* http://www.latimes.com/business/hiltzik/la-fi-hiltzik-20151115-column.html (2015).
9. Tahir, D. *Politico* https://www.politico.com/story/2015/12/drug-companies-data-for-discounts-217080 (2015).
10. Meadows, M. *FDA Consum.* **39**, 18–26 (2005).
11. Walgreens. https://www.walgreens.com/rx-healthanswer/health/p2/a/500001/managing-diabetes-with-walgreens-tools/2414103 (2019).
12. Hummel, P. et al. *Philos. Technol.* **34**, 545–572 (2021).
13. Montgomery, J. *New Bioeth.* **23**, 81–86 (2017).
14. Kukutai, T. & Taylor, J. *Indigenous Data Sovereignty: Toward an Agenda* (ANU Press, 2016).
15. Weichert, T. https://bigbrotherawards.de/en/2021/health-doctolib (2021).
16. Ralston, W. *WIRED* https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/ (2021).
17. Nemitz, P. & Pfeffer, M. in *Regulating Big Tech: Policy Responses to Digital Dominance* (eds. Moore, M. & Tambini, D.) 290 (Oxford Univ. Press, 2021).
18. Pasquale, F. *Law and Political Economy blog* https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/ (2017).
19. Thimmesch, A. B. *Denver Law Rev.* **94**, 145–194 (2016).
20. African Union. https://au.int/sites/default/files/pressreleases/39159-pr-4th_high-level_policy_dialogue_pre-event_pr.pdf (2020).

Competing interests

B.P. is a member of the Austrian National Bioethics Commission and chair of the European Group on Ethics in Science and New Technologies. N.F. is an independent expert member of the Austrian Data Protection Board ('Datenschutzrat'), an advisory body to the government projected in Austrian data protection law, and member of the advisory board to the Austrian COVID-19 data platform. This piece does not represent the opinion of any of these committees. Both authors write in their capacity as researchers and subject experts.