



Protecting Privacy While Optimizing the Use of (Health)Data: The Importance of Measures and Safeguards

Julie-Anne R. Smit, Menno Mostert & Johannes J. M. van Delden

To cite this article: Julie-Anne R. Smit, Menno Mostert & Johannes J. M. van Delden (2022) Protecting Privacy While Optimizing the Use of (Health)Data: The Importance of Measures and Safeguards, The American Journal of Bioethics, 22:7, 79-81, DOI: [10.1080/15265161.2022.2075973](https://doi.org/10.1080/15265161.2022.2075973)

To link to this article: <https://doi.org/10.1080/15265161.2022.2075973>



© 2022 The Author(s). Published with license by Taylor & Francis Group, LLC



Published online: 23 Jun 2022.



Submit your article to this journal [↗](#)



Article views: 1398



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)

OPEN PEER COMMENTARIES

 OPEN ACCESS 

Protecting Privacy While Optimizing the Use of (Health)Data: The Importance of Measures and Safeguards

Julie-Anne R. Smit, Menno Mostert, and Johannes J. M. van Delden

University Medical Centre Utrecht

The possibilities for collecting, storing, and processing of (personal) data have increased significantly over the last decades. It has been argued that an increasing demand for health data will define the future of health research (Ballantyne and Schaefer 2020). But despite the many benefits, at the same time, people are apprehensive about the loss of control, security risks and potential misuse of their data (Street et al. 2021). This has sparked a lively debate among scholars, politicians, policy makers and the public, about the significance of privacy protection and how to cope with the implications of a digitalized world.


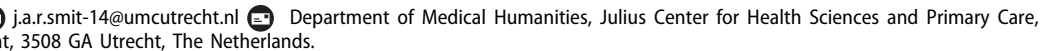
According to Pyrrho, Cambraia, and de Vasconcelos, the privacy-debate is overly framed as a battle between the individual interest and the collective interest, which in their opinion is too simplistic. Since governments have the power to prevent data from being used for discriminatory or unfair purposes, the authors refer to regulatory proposals as “the best solution available” (Pyrrho, Cambraia, and de Vasconcelos 2022). What they do not recognize is that the European legislator has been working on this solution for decades.

The right to privacy (in European law referred to as the right to respect for private life) as well as the right to personal data protection have been acknowledged as fundamental rights and have been adopted into European legislation. Both rights aim to protect similar values. They strive to provide individuals with a personal sphere in which they can think freely and shape their opinions (European Union Agency for Fundamental Rights and Council of Europe 2018).

Nevertheless, the two rights possess different characteristics and should be regarded as separate rights. The “classic” right to respect for private life was originally intended as a negative right, which prohibits interference of public authorities with the private lives of individuals. However, the more “modern” right to data protection is formulated as a predominantly positive obligation, which requires the EU and its Member States to take affirmative measures for the protection of personal data (Mostert et al., 2018).

In recent years, the European legislator has been trying to adopt legislation equipped for a world in which digital technology has become a central part of people’s lives. This has resulted in a modernized version of Convention 108 for the protection of individuals with regard to the processing of personal data, and the introduction of—inter alia—the General Data Protection Regulation (GDPR). The recently proposed Artificial Intelligence Act (AI Act) and the proposed Data Governance Act will complement the landscape of EU legal acts. All of these (proposed) acts contain provisions safeguarding the right to respect for private life and the right to personal data protection.

European data protection legislation is built around several key principles. It requires that the processing of data is lawful, fair, and transparent. In addition, the principles of purpose limitation, data minimization, data accuracy, storage limitation, data security, and accountability must be respected (European Union Agency for Fundamental Rights and Council of Europe 2018). But the data protection legislation also

CONTACT Julie-Anne R. Smit  j.a.r.smit-14@umcutrecht.nl 

© 2022 The Author(s). Published with license by Taylor & Francis Group, LLC

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

contains provisions regarding lawful limitations and justified interferences. The European legislator has acknowledged that the right to respect for private life and the right to data protection are not absolute, that they must be considered in relation to their function in society and be balanced against other fundamental rights.

An example of this balancing can be found in article 9 of the GDPR, which in its first paragraph prohibits the processing of special categories of personal data (such as biometric data and health data). The second paragraph, however, provides for exemptions to this prohibition. Article 9(2)(j) of the GDPR for instance, states that the prohibition does not apply if the processing is necessary for scientific research purposes. When invoking this exemption, it is required to *“provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.”*

As stated in recital 6 of the GDPR, the European legislator aims to *“further facilitate the free flow of personal data [...], while ensuring a high level of the protection of personal data.”* Thus, the rationale is that fundamental rights must be protected, but there are situations in which these rights can be justly interfered with. Interferences should be limited as much as possible by implementing additional measures and safeguards. Examples of such additional measures and safeguards mentioned in the GDPR are pseudonymization and data minimization.

The ideology of “shaping an EU cyberspace based on EU values” (EDPS 2016) is laudable, but putting the ideology into practice has been a complex task. For instance, a recent assessment by the European Commission on the Member States’ rules on health data in light of the GDPR, showed that the margin of appreciation that has been granted to the Member States and which provides them with discretionary powers for the implementation of specific provisions, has caused fragmentation in data protection legislation, standards and guidelines throughout the EU. And because of these differences in implementation and interpretation of the GDPR—e.g. in the area of scientific research—data exchange between Member States and/or EU bodies for research purposes has proven to be challenging (EC 2021).

Alternatively, the proposed AI Act is receiving criticism for not providing adequate protection for fundamental rights and failing to secure legally trustworthy AI (Smuha et al. 2021). Even though according to the European Commission, building an ecosystem of trust is one of the policy objectives

“which should give citizens the confidence to take up AI applications and give companies and public organizations the legal certainty to innovate using AI” (EC 2020).

The collecting, storing, and processing of (personal) data has become part of almost every aspect of people’s lives. Putting these technical developments to a halt—if at all desirable—is impossible. The European Commission has stated that “Europe’s current and future sustainable economic growth and societal well-being increasingly draws on value created by data” (EC 2020). At the same time, in their article, Pyrrho, Cambraia, and de Vasconcelos warn that the conversion of data into economic value is a threat to privacy (i.a.). Consent as well as anonymization are mentioned by the authors as possible means for the protection of privacy. But—together with many other scholars—they acknowledge that those means are not always attainable nor sufficient (Pyrrho, Cambraia, and de Vasconcelos 2022).

Essentially, the European legislator wants to have its cake and eat it too; it wants to optimize the use of (personal) data while safeguarding privacy. The aim is to create a culture in which effectuating data sharing and protecting privacy do not exclude each other but can exist simultaneously. Even when it has become apparent that due to rapid technical developments, some of the “traditional” safeguards such as obtaining consent and anonymizing data are becoming more and more unattainable.

This will have to be resolved with the adaptation of other types of measures and safeguards. Examples mentioned by the Council of Europe are: performing risk assessments, implementing a by design approach and providing education on the implications of the use of information and personal data (COE 2017). Measures and safeguards could furthermore include: oversight by ethics committees or data access committees, engaging the public and enhancing transparency.

Since the field is fast evolving, continuous research should be performed on what the appropriate measures and safeguards are, parallel to the technical and societal developments. Deciding how exactly these measures and safeguards should be implemented is not necessarily a task for the EU legislator. There is room for the Member States, professional groups, or (international) stakeholder collaborations to adapt soft law instruments, such as guidelines or codes of conduct, to effectuate implementation.

Ultimately, the success of the European ideology will be determined by the shaping of the measures and safeguards.

FUNDING

Funding for the work featured in this article was provided by Health~Holland, also known as Stichting LSH-TKI.

REFERENCES

- Ballantyne, A., and G. O. Schaefer. 2020. Public interest in health data research: Laying out the conceptual groundwork. *Journal of Medical Ethics* 46 (9):610–6. doi:10.1136/medethics-2020-106152.
- COE 2017. Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD), Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, Strasbourg, 23 January 2017, T-PD(2017)01.
- EC 2020. European Commission (EC), White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final.
- EC 2021. European Commission (EC), DG Health and Food Safety, Assessment of the EU Member States' rules on health data in the light of GDPR, Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03, Publications Office of the European Union, 2021. doi:10.2818/546193.
- EDPS 2016. European Data Protection Supervisor (EDPS), Opinion 8/2016, EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, 23 September 2016.
- European Union Agency for Fundamental Rights and Council of Europe 2018. European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law* (2018 edition). Publications Office of the European Union, 2018. doi:10.2811/343461.
- Mostert, M., A. L. Bredenoord, B. van der Slootb, and J. J. M. van Delden. 2018. From privacy to data protection in the EU: Implications for Big Data health research. *European Journal of Health Law* 25 (1):43–55. doi:10.1163/15718093-12460346.
- Pyrrho, M., L. Cambraia, and V. F. de Vasconcelos. 2022. Privacy and health practices in the digital age. *The American Journal of Bioethics* 22 (7):50–59. doi:10.1080/15265161.2022.2040648.
- Smuha, N. A., E. Ahmed-Rengers, A. Harkens, W. Li, J. MacLaren, R. Piselli, and K. Yeung, How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission' Proposal for an Artificial Intelligence Act (August 5, 2021). Available at SSRN: <https://ssrn.com/abstract=3899991> or <http://dx.doi.org/10.2139/ssrn.3899991>
- Street, J., B. Fabrianesi, C. Adams, F. Flack, M. Smith, S. M. Carter, S. Lybrand, A. Brown, S. Joyner, J. Mullan, et al. 2021. Sharing administrative health data with private industry: A report on two citizens' juries. *Health Expectations: An International Journal of Public Participation in Health Care and Health Policy* 24 (4): 1337–48. doi:10.1111/hex.13268.

THE AMERICAN JOURNAL OF BIOETHICS
2022, VOL. 22, NO. 7, 81–83
<https://doi.org/10.1080/15265161.2022.2087789>



OPEN PEER COMMENTARIES



Disproof of Concept: Resolving Ethical Dilemmas Using Algorithms

Bryan Pilkington^{a,b} and Charles Binkley^b

^aSeton Hall University; ^bHackensack Meridian Health

Allowing algorithms to guide or determine decision-making in ethically complex situations, and eventually satisfying the need for good clinical ethics consultation work, is a philosophically interesting but wrong-headed endeavor. The fundamental flaw in this approach to ethical decision-making is the assumption that ethical dilemmas are resolved by the judgment of ethics committees and validated by professional ethicists rather than through patient-centered processes.

This flawed assumption leads to three issues which, taken together, are sufficient to reject the proposal. First, an incorrect algorithmic assumption is made, leading to the system being trained on, and validated by, the wrong agents. Second, the account of the professional ethicist that underlies the argument for AI's role in ethically complex situations is misguided. Third, the related assumption, which appears to implicitly motivate the proposal, that medical ethical

CONTACT Bryan Pilkington ✉ bryan.pilkington@shu.edu 📧 Interprofessional Health Sciences and Health Administration, Seton Hall University, 123 Metro Boulevard Nutley, NJ 07110, USA, or Department of Medical Sciences, Hackensack Meridian School of Medicine, 340 Kingsland Street, Nutley, NJ 07110, USA.

© 2022 Taylor & Francis Group, LLC