Zhicheng He (2022): Bridging Law and Technology: Seeing Through Privacy-Enhancing Technologies for Assisted Living from the Perspective of EU Data Protection Law. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Bridging Law and Technology: Seeing Through Privacy-Enhancing Technologies for Assisted Living from the Perspective of EU Data Protection Law

Zhicheng, He
The Swedish Law and Informatics Research Institute, Faculty of Law, Stockholm University
zhicheng.he@juridicum.su.se

Abstract

Our healthcare systems are going through a tide of digital transformation. This is characterised by the increasingly wide use of information and communications technologies (ICT) in various health and care contexts. Early uses of ICT in healthcare focused on digitalising systems that were previously managed manually. One such example is electronic health records (EHRs) which emerged in the 1990s and are now gradually replacing traditional paper-based records (McLoughlin et al. 2017). In addition, a flood of advanced digital technologies is being introduced into healthcare, including artificial intelligence (AI), big data analytics, wearables, sensors for health monitoring, mobile applications, robotics etc. With the advance of ICT, healthcare can even extend from hospital settings to private homes. For example, Active and Assisted Living (AAL) technologies promise to enable older citizens to live more independently in private dwellings, reducing their needs for caregiver interventions (Haque et al. 2020).

Due to the proliferation of ICT in health and care, health data are being collected and processed at an unprecedented scale, with large quantities of health data being stored in EHRs and beyond. Assistive technologies, often seen in the forms of wearables and sensors, can also be privacy-intrusive because they manage user's health and wellbeing status by collecting large quantities of data, such as vital signs, daily activities data and even data of the ambient environment (Ienca and Villaronga 2019). The explosion of health data processing creates two conflicting needs: on one hand, the data privacy of individuals requires the prohibition or minimisation of health data processing; on the other hand, the processing of large quantities of health data is much needed (or even encouraged) to support scientific research, public health management, technological development, among other good purposes.

Privacy-enhancing technologies (PETs) hold the potential to play an important role in reconciling these two conflicting needs by enabling the processing of health data in a less privacy-intrusive manner. Many PETs seek to protect privacy by de-identifying personal data such that natural persons cannot be identified (Ribaric et al. 2016). In the healthcare sector, anonymisation and pseudonymisation represent two groups of commonly used PETs. It should be noted that beyond technical features, anonymisation and pseudonymisation have specific meanings under the EU's data protection legal regime. Rules around these terms have been set out in legal norms, notably the General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union 2016). At the same time, they are important techniques to implement the data protection by design principle, which have become a legal requirement in the EU since the introduction of the GDPR (Tamò-Larrieux 2018).

Despite statutory footings set in the GDPR, the interpretation of anonymisation and pseudonymisation remains far from undisputed. Competing

understandings exist among normative instruments, including the Article 29 Data Protection Working Party's Opinion (Article 29 Working Party 2014), the jurisprudence of the Court of Justice of the European Union, and other guidance issued by national regulators. Beyond the legislative arena, the concept of anonymisation is also hotly debated in academia. Finck and Pallas believe that anonymisation process always comes with a residual risk (Finck and Pallas 2020). Ohm claims that the notion of anonymisation and its privacy protecting power have failed because scientists now have stronger powers to reverse the anonymisation process (Ohm 2009). Rubinstein and Hartzog acknowledge the limitations of anonymisation and argue that the focus should not be placed on preventing harm, but on minimising the risk of re-identification and the disclosure of sensitive attributes through process-based data release policy (Rubinstein and Hartzog 2016). In light of this complexity, Colonna suggests considering synthetic data as an alternative of anonymisation to facilitate health data sharing while acknowledging its potential short comings (Colonna 2020).

Taking a forward-looking perspective, this paper contributes to the scholarly debate around anonymisation and pseudonymisation by extending the discussion to the contexts of forthcoming EU data laws, with a focus on the draft European Health Data Space (EHDS) Regulation (European Commission 2022). It makes preliminary remarks on the role of anonymisation and pseudonymisation in the EHDS Regulation and queries to what extent current legal definitions of anonymisation and pseudonymisation reconcile with data sharing arrangements proposed by this up-coming EU data regulation. This paper observes that ongoing debates do not seem to have affected EU policy makers in affording more weight on anonymisation and pseudonymisation. Rather, the EHDS Regulation requires health data to be shared only on an anonymised or pseudonymised basis. It seems therefore reasonable to expect anonymisation and pseudonymisation to play a core role in the EU's future health data sharing framework. This paper further argues that an EU level guidance on anonymisation and pseudonymisation in light of the new legal framework is still much needed, such that the privacy-enhancing powers and data sharing facilitation potentials of these techniques could be unleashed to a greater extent.

Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 861091. The publication reflects the views only of the authors, and the European Union cannot be held responsible for any use which may be made of the information contained therein.

References

Article 29 Working Party. 2014. Opinion 05/2014 on Anonymisation Techniques.

Colonna, Liane. 2020. Privacy, Risk, Anonymization and Data Sharing in the Internet of Health Things. Pittsburgh Journal of Technology Law & Policy 20. https://doi.org/10.5195/tlp.2020.235.

European Commission. 2022. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final.

European Parliament, and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Vol. Regulation (EU) 2016/679.

Finck, Michèle, and Frank Pallas. 2020. They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law 10: 11–36. https://doi.org/10.1093/idpl/ipz026.

Haque, Albert, Arnold Milstein, and Li Fei-Fei. 2020. Illuminating the dark spaces of healthcare with ambient intelligence. Nature 585: 193–202. https://doi.org/10.1038/s41586-020-2669-y.

Ienca, Marcello, and Eduard Fosch Villaronga. 2019. Privacy and Security Issues in Assistive Technologies for Dementia: The Case of Ambient Assisted Living, Wearables, and Service Robotics. In Intelligent Assistive Technologies for Dementia: Clinical, Ethical, Social, and Regulatory Implications, 221–239. Oxford University Press.

McLoughlin, Ian, Karin Garrety, Rob Wilson, Ping Yu, and Andrew Dalley. 2017. The digitalization of healthcare: electronic records and the disruption of moral orders. First edition. Oxford ; New York, NY: Oxford University Press.

Ohm, Paul. 2009. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review 57: 1701–1778.

Ribaric, Slobodan, Aladdin Ariyaeeinia, and Nikola Pavesic. 2016. De-identification for privacy protection in multimedia content: A survey. Signal Processing: Image Communication 47: 131–151. https://doi.org/10.1016/j.image.2016.05.020.

Rubinstein, Ira S., and Woodrow Hartzog. 2016. Anonymization and Risk. Washington Law Review 91: 703–760.

Tamò-Larrieux, Aurelia. 2018. Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things. Vol. 40. Law, Governance and Technology Series. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-98624-1.