Privacy-enhancing Technologies for Active and Assisted Living: What Does the GDPR Say?

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

ABSTRACT

Privacy-enhancing technologies (PETs) promise to safeguard privacy and security alongside the use of active and assisted living (AAL) tools. To what extent PETs meet the expectations of EU data protection norms however needs to be better understood. This paper aims to determine whether PETs used for AAL purposes are anonymisation or pseudonymisation methods under the General Data Protection Regulation (GDPR). In this paper, doctrinal legal research is used as the main research method. This means that primary legal sources such as EU laws will be relied upon and analysed in the context of PETs for AAL purposes. Specifically, this paper first conducted an inquiry into several important EU data protection concepts, namely anonymisation, pseudonymisation and data protection by design. On this basis, focus was shifted to state-of-the-art PETs for AAL, which are then used as examples to measure against these data protection concepts. A closer look at PETs in the AAL context finds that most groups of PETs for AAL are more likely to be considered as pseudonymisation methods rather than anonymisation methods because of their technical reversibility. This general assessment is however subject to change in each specific case since the notion of anonymisation under the GDPR is not absolute, but contextual specific and sensitive to factors such as costs, time, and available technologies for re-identification. Based on the findings, clearer guidance seems necessary in order to determine what constitutes anonymisation under the EU data protection regime such that legal certainty could be increased.

KEYWORDS

Data protection by design, GDPR, Privacy-enhancing technologies, Active and assisted living, Anonymisation, Pseudonymisation

ACM Reference Format:
Zhicheng, He. 2022. Privacy-enhancing Technologies for Active and Assisted Living: What Does the GDPR Say?. In *The15th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA '22), June 29–July 01, 2022, Corfu, Greece.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3529190.3534719

1 INTRODUCTION

Statistics send us a warning that our societies are ageing rapidly [14]. This trend poses serious threats to the sustainability of our healthcare systems globally. Emerging assistive technologies, such as Active and Assisted Living (AAL) technologies, promise to relieve this ageing crisis by enabling older citizens or other people in need to live more independently and longer in their private dwellings, reducing needs for caregiver interventions [9]. However, these assistive technologies, seen in the forms of wearables and sensors, can 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 data of the ambient environment.

Along with the increasing awareness of personal data protection, privacy-enhancing technologies (PETs) are being developed and implemented to enhance user privacy accompanying the use of information systems. PETs seek to protect privacy by de-identifying personal data, such that personal data is rendered 'anonymous' and natural persons cannot be identified [13]. It remains however unclear where do PETs stand under the EU data protection regime. Yet this may be extremely difficult. As illustrated below, this is partly due to the technical complexity of PETs, and partly because of the ambiguity that exists in the EU data protection norms.

Given this context, this paper aims to determine the relations between PETs for AAL purposes and some important EU data protection concepts. First, this paper seeks to examine the meaning of anonymisation and pseudonymisation under the EU General Data Protection Regulation (GDPR) [6]. On the basis of this legal analysis, focus is then shifted to state-of-the-art PETs in the AAL field, which are used as examples to measure against fundamental EU data protection concepts (anonymisation, pseudonymisation and data protection by design) to determine whether they are anonymisation methods or pseudonymisation methods under the GDPR (sections 3 and 4).

2 THE LAW

In Europe, the right to privacy is enshrined in two important treaties, namely the EU's Charter of Fundamental Rights of the European Union (CFR) [7] and Council of Europe's European Convention for Human Rights (ECHR) [3]. Article 8 of the CFR states that 'Everyone has the right to respect for his private and family life, his home and his correspondence' [7]. Similarly, Article 7 of the ECHR stipulates that 'Everyone has the right to respect for his or her private and family life, home and communications' [3]. The scope of the right to privacy should not be understood restrictively. According to the jurisprudence of the European Court of Human Rights, the right to privacy covers, among other, the protection of personal data, secrecy of correspondence, protection of domicile, and bodily integrity [8].

The adoption of the GDPR further harmonised data protection rules in the EU. For developer of information technologies, it is important to note that data protection by design and default has

PETRA '22, June 29–July 01, 2022, Corfu, Greece

ACM ISBN 978-1-4503-9631-8/22/06.
https://doi.org/10.1145/3529190.3534719

now become a legal requirement in the EU [6]. The GDPR also sheds light on important data protection concepts such as anonymisation and pseudonymisation. To understand the relations between PETs for AAL and EU data protection norms, relevant rules of the GDPR therefore serve as an important starting point.

2.1 Anonymisation

Anonymisation is generally understood as the process that renders personal data anonymous [5]. To further determine the legal definition and requirements of anonymisation under the EU data protection regime, the concept of personal data is central. GDPR defines personal data as 'any information relating to an identified or identifiable natural person' [6]. Following this logic, information that does not relate to any identified or identifiable natural person is not personal data, ie anonymous information. In fact, the GDPR did provide a reference to anonymous information to this effect. Under the GDPR, anonymous information is referred to as 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable' [6].

Accordingly, there are two types of anonymous information: (1) information that is not related to any identified or identifiable natural person; (2) information that was originally personal data but is then rendered anonymous such that natural persons are no longer identifiable. The second category is closely related to PETs used in the AAL context because many of these techniques aim to render personal data not identifiable, or at least more difficult to be identified [12].

An important question is how to determine whether natural persons are still identifiable after being processed by PETs. This is not only key from a technical perspective, but also vital in distinguishing personal data and anonymous information given their significantly different legal implications: personal data is subject to rules of the GDPR, whereas anonymous information falls outside the scope of the GDPR because it is not considered personal data [6].

The GDPR provides further guidance in this regard. First, to ascertain whether a natural person is identifiable, it is important to consider 'all the means reasonably likely to be used' by other parties to identify that natural person [6]. Further, to determine what means are reasonably likely to be used by such other parties to identify people, all objective factors must be considered, including (1) the costs for identification, (2) the time required for identification, (3) the available technology at the time of the processing and (4) technological developments [6].

2.2 Pseudonymisation

Another important and relevant concept is pseudonymisation, with its legal definition clearly given in Article 4(5) of the GDPR. According to the GDPR, pseudonymisation means 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information' [6]. The GDPR also provides additional requirements for pseudonymisation and requires that such 'additional information' must be kept separately, and technical and organisational measures must be taken to prevent re-identification [6].

Under the GDPR regime, pseudonymisation is vastly different from anonymisation. Unlike anonymisation, pseudonymisation is generally understood as a reversible process, as indicated in its definition. This means that with the help of additional information, pseudonymised information may be reversed to enable the re-identification of natural persons. In this sense, pseudonymised personal data is still governed by and subject to the requirements of the GDPR because it is still considered personal data. However, anonymous information is out of the jurisdiction of the GDPR because it is not personal data [6].

2.3 Data Protection by Design

Despite major differences, both pseudonymisation and anonymisation are important measures to implement the 'data protection by design' principle. GDPR has made clear that pseudonymisation is an important means of implementing the principle of 'data protection by design' [6]. While GDPR did not directly refer anonymisation as an example of data protection by design, it is also a vital way to achieve the purposes of data protection by design given that anonymisation should be a more irreversible process than pseudonymisation. Data protection by design principle requires data controllers to take technical and organisational measures and necessary safeguards into the processing of personal data, such that data protection principles are implemented and that the rights and freedoms of data subjects are protected [4]. As stipulated in Article 5 of the GDPR, data protection principles include transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, accountability, etc [6].

In addition to data protection by design, GDPR also introduces another requirement called 'data protection by default'. Data protection by default requires data controllers to implement appropriate technical and organisational measures to ensure that, by default, only necessary data is processed [6].

3 PRIVACY-ENHANCING TECHNOLOGIES FOR AAL

With concepts like 'privacy by design' and 'data protection by design' becoming popular in recent decades, many PETs have been developed and proposed to enhance privacy. For example, researchers have provided a categorisation of visual privacy preservation methods that could be used to enhance visual privacy, including intervention methods, blind vision, secure processing, data hiding, and redaction methods [10]. Other researchers summarised de-identification of personal identifiers in multimedia contents, including non-biometric personal identifiers, biometric personal identifiers, and soft-biometric personal identifiers [13].

More recently, Ravi, Climent-Pérez, and Florez-Revuelta have provided an updated taxonomy by reviewing state-of-the-art visual privacy protection methods for AAL, with a focus on visual obfuscation methods and biometric identifiers in private settings, such as gait, gestures, actions, dressing styles and activities [12]. This taxonomy divides relevant PETs into five groups, namely intervention methods, blind vision methods, secure processing methods, data hiding methods and obfuscation methods [12]. Each group of methods has its unique feature. Intervention methods refer to techniques that prevent private visual data from being collected in the

data collection phase, including sensor saturation (such as privacy stickers for laptop and phone cameras), broadcasting commands (which is less effective and popular as compared with sensor saturation methods) and context-based approaches [11]. Blind vision methods rely on the use of secure multi-party computation (SMC) encryption techniques, which were referred to as the processing of images and videos in an anonymous way [2]. Methods that are not based on SMC but rely on encryption for privacy preservation are categorised under the group of 'secure processing' [12]. Data hiding methods refer to techniques that protects privacy by modifying original data in a way that embeds original information underneath the modified information, such that the original information can be restored if necessary [12]. Obfuscation methods are divided into two sub-groups: perceptual obfuscation, and machine obfuscation. Perceptual obfuscation methods target human observers by making the privacy-sensitive elements in the images perceptually different for them. Techniques used include image filtering, facial de-identification, total body abstraction, gait anonymisation and environment replacement. These techniques can be either reversible or irreversible [12]. Machine obfuscation methods create changes in images to protect the privacy of users from the recognition of machine learning algorithms [12]. In the following section, this taxonomy is used as a framework to discuss the relations between PETs for AAL and EU data protection laws.

4 DISCUSSION

Measures required by the 'data protection by design' principle should be understood broadly as to include any measures data controllers might use in data processing. One notable such example is the pseudonymisation of personal data, which is specifically mentioned in the GDPR [6]. In this sense, PETs could be used as approaches to materialise the 'data protection by design' requirements of the GDPR.

To further determine the possible legal positions of PETs, connections between PETs and the concept of anonymisation and pseudonymisation need to be explored. As discussed above, reversibility is the most important distinction between anonymisation and pseudonymisation. In this sense, anonymisation represents de-identification processes that are not reversible, whereas pseudonymisation refers to de-identification processes that are reversible.

Accordingly, intervention methods are more likely to be placed into the anonymisation group. This is however not because intervention methods render personal data anonymous, but because these methods prevent the collection of sensitive personal data in the first place, ie during the data collection phase. If personal data was not collected in the beginning, then the information collected would more likely be anonymous because it would not relate to any identified or identifiable natural person.

The following three groups of PETs for AAL, ie blind vision, secure processing and data hiding methods, are more likely to be recognised as pseudonymisation methods because of their possible reversibility. While Avidan and Butmar refer to 'blind vision' methods as methods that process images and videos in an anonymous way [2], their legal status are more similar to pseudonymisation methods under the EU data protection legal regime because most of these methods were designed to be reversible [12]. The same categorisation applies to secure processing methods because they are reversible in many cases [12]. Data hiding methods are more likely to regarded as pseudonymisation methods because these methods function by embedding original information underneath the modified information. This means that original information could be restored when necessary [12].

The last group, visual obfuscation methods, is more complex. This group contains methods that are reversible and irreversible (such as total body abstraction). Therefore, methods under this group need to be examined in more detail to determine their legal status.

A general analysis focusing on the technical reversibility of visual privacy preservation methods demonstrates that, while intervention methods ensure anonymisation, the remaining four groups of techniques are more likely to be considered as pseudonymisation methods (with the exception of a few methods under the visual obfuscation group which are technically irreversible). But this analysis may be complicated by the relativity of anonymisation under EU data protection norms, notably the GDPR. The GDPR provides that the determination of identifiability depends on contextual factors such as time, money and technologies that may be used to reverse such information. This indicates that in real life, PETs that are technically reversible could potentially render anonymisation because the reversibility may in fact be impossible for organisations to achieve without enough means available to these organisations.

Further, while this paper focuses on the notion of anonymisation under the GDPR, results of the analysis above may become more complicated when broader EU data protection norms are considered, such as Article 29 Data Protection Working Party's Opinion on anonymisation techniques [1]. The tension between relevant EU laws, guidance, case law and literature around what constitutes anonymisation is complex and needs to be addressed in separate papers.

5 CONCLUSIONS

This paper aims to bring together PETs for AAL and EU data protection laws and determine the relationships between them. For this purpose, PETs in the AAL context are used as examples to measure against fundamental EU data protection concepts, namely anonymisation, pseudonymisation and data protection by design. A closer look at PETs in the AAL context finds that most groups of PETs are more likely to be considered as pseudonymisation methods rather than anonymisation methods because of their technical reversibility. This general assessment is however subject to change in each specific case since the notion of anonymisation under the GDPR is not absolute, but contextual specific and sensitive to factors such as costs, time, and available technologies for re-identification. Based on the findings, clearer guidance seems necessary in order to determine what constitutes anonymisation under the EU data protection regime such that legal certainty could be increased.

ACKNOWLEDGMENTS

The author wishes to thank Prof Martin Kampel and colleague Siddharth Ravi for their comments and generous help. 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.

REFERENCES

[1] Article 29 Working Party. 2014. Opinion 05/2014 on Anonymisation Techniques. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[2] Shai Avidan and Moshe Butman. 2006. Blind Vision. In Computer Vision – ECCV 2006 (Lecture Notes in Computer Science), Springer, Berlin, Heidelberg, 1–13. DOI:https://doi.org/10.1007/11744078_1

[3] Council of Europe. 1950. European Convention on Human Rights. Retrieved March 9, 2022 from https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c

[4] EDPB. 2020. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

[5] EDPS and AEPD. 2021. AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en

[6] 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). Retrieved February 5, 2022 from https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] European Union. 2012. Charter of Fundamental Rights of the European Union. Retrieved March 9, 2022 from http://data.europa.eu/eli/treaty/char_2012/oj/eng

[8] Raphaël Gellert and Serge Gutwirth. 2013. The legal construction of privacy and data protection. Computer Law & Security Review 29, 5 (October 2013), 522–530. DOI:https://doi.org/10.1016/j.clsr.2013.07.005

[9] Albert Haque, Arnold Milstein, and Li Fei-Fei. 2020. Illuminating the dark spaces of healthcare with ambient intelligence. Nature 585, 7824 (September 2020), 193–202. DOI:https://doi.org/10.1038/s41586-020-2669-y

[10] José Ramón Padilla-López, Alexandros Andre Chaaraoui, and Francisco Flórez-Revuelta. 2015. Visual privacy protection methods: A survey. Expert Systems with Applications 42, 9 (June 2015), 4177–4195. DOI:https://doi.org/10.1016/j.eswa.2015.01.041

[11] Alfredo J. Perez, Sherali Zeadally, and Scott Griffith. 2017. Bystanders' Privacy. IT Professional 19, 3 (2017), 61–65. DOI:https://doi.org/10.1109/MITP.2017.42

[12] Siddharth Ravi, Pau Climent-Pérez, and Francisco Florez-Revuelta. 2021. A Review on Visual Privacy Preservation Techniques for Active and Assisted Living. arXiv: 2112.09422 [cs] (December 2021). Retrieved January 13, 2022 from http://arxiv.org/abs/2112.09422

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

[14] United Nations. 2020. World population ageing 2020 Highlights: living arrangements of older persons. United Nations. Retrieved May 7, 2021 from https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/undesa_pd-2020_world_population_ageing_highlights.pdf