Article:
Piasecki, S., Chen, J. orcid.org/0000-0002-1970-6762 and McAuley, D. (2022) Putting the right P in PIMS: normative challenges for protecting vulnerable people's data through personal information management systems. European Journal of Law and Technology, 13 (3). ISSN 2042-115X

EJLT European Journal of Law and Technology

Putting the Right P in PIMS: Normative Challenges for Protecting Vulnerable People's Data through Personal Information Management Systems

Stanislaw Piasecki,[*] Jiahong Chen[**] & Derek McAuley[***]

Abstract

An increasing number of vulnerable individuals live within smart homes. Personal information management systems (PIMS) are a type of privacy enhancing technology (PET), which could help in safeguarding and managing their data more efficiently within a smart home context, thereby improving compliance with data protection law. Using PIMS for protecting vulnerable people's personal data, however, may raise questions regarding the normative justifications for this technological approach. The extra care and support owed to individuals with vulnerabilities may tip the balance in some theoretical debates, such as 'privacy as confidentiality vs privacy as control'. By further examining these debates in the context of IoT devices used by vulnerable people, it is shown that while edge-computing PIMS hold promise for enhancing privacy protection for vulnerable data subjects, designers of these systems need to consider carefully the implications of implementing different privacy paradigms.

Keywords: compliance, PIMS, technologies, GDPR, IoT, vulnerable

[*] Dr Stanislaw Piasecki (https://orcid.org/0000-0001-5748-8631), s.piasecki@uva.nl, Institute for Information Law, University of Amsterdam.
[**] Dr Jiahong Chen, Lecturer in Law, School of Law, University of Sheffield.
[***] Prof Derek McAuley, Professor of Digital Economy and Director of Horizon Digital Economy Research, Faculty of Science, University of Nottingham.

1. Introduction

One of the main goals of privacy enhancing technologies (PETs) is to enable personal data processing and provide answers to data queries without allowing third parties to gain access to the whole of the data.[1] This emerging and innovative group of technologies, together with recent and on-going alterations in wider business and policy structures, could allow remarkably greater sharing and processing of data in a more privacy-preserving and trust-building way. New possibilities to explore datasets could be developed, leaving behind the unacceptably high levels of risks associated with current data processing practices. This article evaluates how the relationship between smart home devices, personal data and vulnerable people can be reshaped through a particular category of PETs, namely personal information management systems (PIMS), in order to better protect vulnerable individuals' data and facilitate data protection compliance. It strives to understand how to bridge the gap between law in theory and law in practice by using PIMS. Theoretically, the nature and merits of privacy will be clarified in relation to underlying debates such as privacy-as-confidentiality versus privacy-as-control or cloud-based data processing versus edge-based systems.

In terms of the definition of vulnerable people, this paper focuses on children and also adults subject to commonly accepted cognitive disabilities, although we acknowledge the need to further explore the boundaries of vulnerable data subjects in a smart home context.[2] This has the advantage of underlining the most serious general challenges and being able to analyse more broadly how they could be tackled by PIMS in order to better protect vulnerable people's data and support organisations' data protection law compliance.

This article chooses domestic IoT – or commonly known as smart home technologies – as the case study not just because this is an emerging area where many legal

[1] The Royal Society, 'Protecting Privacy in Practice. The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis' (March 2019) <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf> accessed 1 November 2022.

[2] Luna states that everyone is vulnerable but some of us have more vulnerability layers than others. (See Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2(1) International Journal of Feminist Approaches to Bioethics 121.) This layered perspective seems to be in conformity with GDPR's risk-based approach, which also indicates that any person can be vulnerable but at different levels and that situations may vary. This study focuses on children and adults who are inherently vulnerable, that is whose layers of vulnerability exist continuously and indisputably, such as adults with disabilities in line with the ECtHR's jurisprudence. (See Alexandra Timmer, 'Vulnerability: Reflections on a New Ethical Foundation for Law and Politics' in Martha Albertson Fineman and Anna Grear (eds), *A Quiet Revolution: Vulnerability in the European Court of Human Rights* (Ashgate 2013); Alexandra Timmer, 'Strengthening the Equality Analysis of the European Court of Human Rights: The Potential of the Concepts of Stereotyping and Vulnerability' (Doctor of Law, Universiteit Gent 2014).

issues arise,[3] but also because, as will be shown throughout this paper, it highlights the difficulties in applying privacy and data protection theories developed in pre-smart home times to this new socio-technical reality. An increasing number of vulnerable people will use IoT products in their homes for purposes such as entertainment or health tracking. For this reason, it is crucial to analyse technology that can support vulnerable persons' data protection and control in a smart home context.

The main objective of this paper is to show the potential (and challenges, which need to be tackled to realise this potential) of edge-computing PIMS in enhancing data protection law compliance when vulnerable people use smart devices. To do so, this article firstly discusses the necessity to take vulnerable people's data protection needs into consideration, defines PIMS and argues in favour of edge computing in the context of the cloud versus edge debate. Subsequently, it analyses how PIMS should address the issue of managing data when vulnerable people use smart products. Finally, it considers when confidentiality or control should be prioritised as well as practical capabilities of edge-computing PIMS to enable better GDPR compliance in terms of security and data minimisation.

2. Edge-Based PIMS as a Technical Model

2.1 Taking Vulnerable People's Data Protection Needs into Consideration

Data protection by individuals, also called 'do-it-yourself' data protection, is often seen as an essential part of effective and comprehensive data protection strategies.[4] However, the wide-spread and meaningful adoption of 'do-it-yourself' data protection practices is quite unlikely. For this to change, data protection would need to be a 'collective, profoundly political endeavour'.[5] At the moment, effectively protecting data on the internet is still a skill that few people possess. It requires knowledge of various applications and software, not accessible to every member of society. In the long-lasting discussion related to the 'digital divide', some commentators have blamed the 'information have-nots' and 'laggards' who lack knowledge or resources instead of focusing on the actual structural reasons for

[3] See, for example, Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR when Vulnerable People use Smart Devices' (2022) International Data Privacy Law; Lisa Collingwood, 'Villain or Guardian? "The Smart Toy is Watching You Now … ."' (2021) 30(1) Information & Communications Technology Law 75; Ingrida Milkaite and Eva Lievens, 'The Internet of Toys: Playing Games with Children's Data?' in Giovanna Mascheroni and Donell Holloway (eds), *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Play* (Palgrave Macmillan 2019).

[4] Tobias Matzner and others, 'Do-It-Yourself Data Protection - Empowerment or Burden?' in Serge Gutwirth, Leenes Ronald and Paul De Hert (eds), *Data Protection on the Move Law, Governance and Technology Series*, vol 24 (Springer, Dordrecht 2016).

[5] Matzner (n 4).

inequalities in this field.[6] Such assertions ignore the needs of those who require the most protection in a smart home context – children and vulnerable adults.

In some cases, data protection is becoming an expensive product feature while in others it is only attainable to those who possess substantial information on this topic. Moreover, certain groups (for example, due to their old age or being a child) face the risk of discrimination or social stigma and, therefore, their data protection needs require additional attention to those of other citizens.[7] Barriers to comprehending consequences of how their data is shared and what are actual users' choices often prevent them from making informed decisions. Solove considers that self-management of privacy does not give individuals meaningful control over their personal data, one of the problems being severe cognitive issues (lack of knowledge and skewed decision-making) that compromise privacy self-management.[8] Those issues diminish people's capacity to make informed decisions related to the risks and potential benefits of consenting to the processing of their data, and could be exacerbated in the context of some vulnerable individuals. Furthermore, according to Solove, even well-informed persons cannot effectively self-manage their data as 'there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity'.[9] Again, such problems will manifest themselves even more severely when it comes to data subjects with vulnerabilities. However, this does not mean that self-management must be completely abandoned. It should be done in a way that both empowers individuals and protects them at the same time while facilitating legal compliance.

2.2 A Rising Interest in PIMS

The General Data Protection Regulation (GDPR) [10] has several provisions the objective of which is to increase vulnerable people's data protection (children are mentioned in Rec. 38, 58, 65, 71, 75, Art. 6.1 (f), 8, 12, 40.2 (g) and 57.1 (b) and vulnerable persons in general (in Rec. 75). Read in combination with the requirement of data protection by design (Art. 25 GDPR), this would mean data controllers are required to take proper technical measures to provide such protection to vulnerable data subjects. Technical solutions are sometimes more effective to offer protection to data subjects. As Hildebrandt suggests, a 'possible solution to the systemic gaps in legal protection is to use technology itself to enforce

[6] Matzner (n 4).
[7] Matzner (n 4).
[8] Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126(7) Harvard Law Review 1880, 1880–1881.
[9] Solove (n 8).
[10] 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, 'GDPR'), [2016] OJ L 119/1.

legal rules'.[11] The ambient intelligence in smart home environments based on real time monitoring of data subjects requires the adoption of both legal and technology tools to counter the asymmetry of power that it creates, even more so in relation to vulnerable people.[12]

A number of technical solutions have been developed under the name of privacy enhancing technologies (PET) to foster more accountable and effective personal data processing, frequently in the context of complying with privacy by design[13]. The UK Royal Society's report on privacy enhancing technologies has identified five PETs as the most promising ones in terms of their potential to promote privacy-preserving data processing, namely personal information management systems (PIMS), differential privacy, homomorphic encryption, trusted execution environments and secure multi-party computation.[14] While all of the PETs mentioned by the Royal Society report have high potential to support GDPR compliance, PIMS are particularly relevant in the context of smart homes and the processing of vulnerable people's personal data in this setting as they strive to provide security, data management solutions and opportunities for users to take decisions in relation to their data. PIMS can take the form of 'physical box-sets or apps on for instance phones or tablets' which can be enhanced by various types of PETs.[15] Solid, for example, is a MIT project led by Prof. Tim Berners-Lee, which allows users to 'control which entities and apps can access their data through Solid Pods' (the latter being decentralised data stores providing data subjects with 'permissioning controls').[16]

PIMS are considered to hold promise to enable vulnerable users to exercise their rights under the GDPR. They provide people with the opportunity to decide who they wish to trust with the data they produce.[17] Current practices of IoT companies often lead to clear GDPR violations such as the lack of transparently communicated information, obscure consent mechanisms, gathering data by default instead of protecting by default, lack of strong security mechanisms, lack of data protection impact assessments (even though they are required for vulnerable people using smart products) and undermined data minimisation through transfers of large quantities of personal data to the cloud.[18] PIMS are designed to address some of

[11] Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) Modern Law Review 428, 443.
[12] Mireille Hildebrandt, 'Profiling and the Rule of Law' (2008) 1(1) Identity in the Information Society 55.
[13] Claudia Diaz, Omer Tene and Seda Gurses, 'Hero or Villain: the Data Controller in Privacy Law and Technologies' (2013) 74(6) Ohio State Law Journal 923.
[14] The Royal Society (n 1).
[15] The Royal Society (n 1).
[16] Solid, 'What is Solid?' (2020) <https://inrupt.com/solid/> accessed 1 November 2022.
[17] The Royal Society (n 1).
[18] Lachlan Urquhart, Andy Crabtree and Tom Lodge, 'Demonstrably Doing Accountability in the Internet of Things' (2018) 27(1) International Journal of Law and Information Technology 1; Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and

those issues. They are not just tools for more privacy-preserving data processing and do not only focus on security and enforcement like many other PETs, but take into consideration the aforementioned mechanisms from the standpoint of new privacy paradigms. Indeed, PIMS are platforms providing 'the means and infrastructure for mediating between users and those seeking to process their data'.[19] They strive to give consumers more control over how their personal data is managed (as required by the GDPR).

Art. 32 GDPR mandates the adoption of organisational and technical measures to develop more secure systems that reduce the risks to individuals' rights and freedoms. The choice of the technical and organisational measures lies with the controller. The use of the word 'appropriate' signifies that the controller maintains discretion as to the measures and procedures they will implement.[20] PIMS could be an effective technology to help companies in meeting their data protection compliance needs. Depending on where the user's data is stored, PIMS can be categorised as cloud- or edge-based. As will be shown in the next sub-section, the increasing popularity of PIMS could see a shift from a cloud-based to an edge-based approach to data processing.

2.3 The Cloud Computing and Edge Computing Approaches

Cloud offerings are presented by some authors as providing an enhanced user experience 'driven by self-service, simplification, standardization, economies of scale, and technology advancement'.[21] Many services that consumers use to download apps or store their media are hosted by cloud systems, especially in the IoT field. A mix of three fundamental concepts define the cloud's objectives: 'the first is delivering a service, such as computing or storage as a utility; the second is multiple people sharing the same computer resource, referred to as virtualisation; the third is accessing services via networking'.[22] However, recent technological developments now also allow edge solutions – those shifting processing activities to terminal devices, the edge of the internet – to achieve those three objectives. In some cases, the edge even offers better quality of service and experience for applications that need real-time response as data does not need to travel to geographically distant cloud data centres.[23] There are various PIMS currently in

---

Demonstrating their Influence' (CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, April 2020).

[19] Heleen Janssen and others, 'Decentralized Data Processing: Personal Data Stores and the GDPR' (2021) 10(4) International Data Privacy Law 356.

[20] Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29(5) Computer Law & Security Review 509.

[21] Juhnyoung Lee, 'A View Of Cloud Computing' (2013) 1(1) International Journal of Networked and Distributed Computing 2.

[22] Blesson Varghese, 'A History of the Cloud' (2019) 61(2) ITNOW 46.

[23] Blesson Varghese and others, 'Challenges and Opportunities in Edge Computing' (IEEE International Conference on Smart Cloud (SmartCloud), New York, November 2016).

development, both edge-computing and cloud-based, such as midata,[24] DigiMe[25] or the previously mentioned Solid[26] (and many others). The opposing architectural models in these two approaches mean that they might perform differently in facilitating compliance with the GDPR and protecting vulnerable individuals' data.

Cloud systems run applications in a centralised manner. When using this architecture, smart devices transfer the data they generate to central servers for processing. Companies implementing centralised approaches presume that consumers do not dispute the integrity of the hosting company (and the honesty of those who work for this company) nor its capabilities in terms of protecting against acute threats such as honeypots (creating economic incentives for hackers).[27] Edge architectures, by contrast, are capable of offering similar benefits to cloud-based systems with improved privacy. The user-based edge model uses local data processing instead of transferring raw data to a central node. It allows for the creation of a distributed system, where personal data processing and storage takes place at the edge of the network, instead of being centralised. With the increasing computing power of terminal devices, resource-demanding components of the system, such as machine learning algorithms, can now travel to the local data rather than the locally collected data travelling to the algorithms on remote servers.[28]

One example of a system that processes data at the edge of the network is the Databox project.[29] This is a prototype edge-computing platform with a physical device placed in a person's house and data gathered by smart products transferred into this system after primary usage.[30] It can be defined as 'a protective container for personal data where data may actually be located in different geographical locations [and it] will act as a virtual boundary (or as a gatekeeper) where it controls how, when, what data is shared with external parties'.[31] Databox offers methods inspired by the Human-Data Interaction (HDI) model to allow people to comprehend what kind of data is collected about them and the manner in which it is processed.[32] The system is founded on isolating the raw personal data stores from other stores

[24] midata, 'My Data – Our Health' (2021) <https://www.midata.coop/en/home/> accessed 1 November 2022.
[25] digi.mi, 'What is digi.me?' (2021) < https://digi.me/> accessed 1 November 2022.
[26] Solid (n 16).
[27] Nicolas Anciaux and others, 'Personal Data Management Systems: The Security and Functionality Standpoint' (2019) 80 Information Systems 13.
[28] The Royal Society (n 1).
[29] Urquhart, Crabtree and Lodge (n 18).
[30] Charith A. Perera and others, 'Valorising the IoT Databox: Creating Value for Everyone' (2016) 28(1) Trans Emerging Telecommunications Technologies 1.
[31] Perera and others (n 30).
[32] Richard Mortier and others, 'Human-Data Interaction: The Human Face of the Data-Driven Society' (*arXiv:1412.6159*, 6 January 2015) <https://arxiv.org/abs/1412.6159> accessed 1 November 2022; Amir Chaudhry and others, 'Personal Data: Thinking Inside the Box' (2015) 1(1) Aarhus Series on Human Centered Computing 4.

devoted to presenting aggregated query results, which can be transferred to remote third parties.[33]

In addition to other benefits (and potential issues) linked to edge-computing systems, edge-computing solutions, above all, have the advantage of ensuring the integrity and confidentiality of IoT users' data. However, switching to the edge would require disrupting current business models, which will of course lead to resistance as many organisations rely on the economic benefits of centralised cloud architectures. Widespread adoption of this new model requires 'a critical mass of uptake that would provide confidence to other consumers and businesses' that PIMS are worth using.[34] One way to do so would be for governments to lead by example, promote and use such products, and let companies as well as consumers learn from their experience to gain trust in the edge.

Another potential barrier to the adoption of edge-based systems is the lack of interoperability of IoT devices and the existence of technological silos within which users are forced to operate when they buy smart products. Solid is an example of a PIMS project that strives to achieve interoperability as 'all data in a Solid Pod is stored and accessed using standard, open, and interoperable data formats and protocols'.[35]

With the data protection benefits of edge-based PIMS, there is a strong case for governments to promote this approach by supporting the industry to overcome commercial and technical barriers. When deploying such solutions, however, organisations also need to address the special needs of vulnerable data subjects, which is something under-discussed in the literature at the moment.

3. Managing Vulnerable People's Data Collected by Smart Devices

3.1 Supporting Vulnerable Individuals in Securely Controlling their Own Data

The majority of people using products such as IoT devices are not opting out as companies process their personal data. They are 'exposing the intimate minutiae of their lives on sites like Facebook and Twitter', as well as through smart products.[36] However, this rise in sharing data is not only the consequence of people's choices but also, in part, a consequence of the fact that numerous smart devices are

[33] Anciaux and others (n 27).
[34] The Royal Society (n 1); Guillaume Brochot and others, 'Study on Personal Data Stores conducted at the Cambridge University Judge Business School' (*European Commission,* 7 August 2015) < https://digital-strategy.ec.europa.eu/en/library/study-personal-data-stores-conducted-cambridge-university-judge-business-school> accessed 1 November 2022.
[35] Solid, 'Fully Interoperable Standards' (2021) <https://solidproject.org/> accessed 1 November 2022.
[36] Solove (n 8) 1895.

designed in a way that promotes data sharing and limits understanding of the risks involved. This issue is made even more acute because of the many children, teenagers and vulnerable adults whose capacity to make informed choices may be lower than that of other citizens. One of the main objectives of PIMS is to allow the user to take more meaningful decisions concerning the dissemination of their personal data.[37] PIMS are making it possible for consumers to determine which personal computations they will give permission for and which collective computations they will agree to participate in.

In the PIMS smart home context, the responsibility of taking appropriate decisions and their enforcement falls on users of smart devices. This leads to risks for vulnerable people. Some authors argue that 'we should be cautious of a potential boomerang effect of user empowerment' when giving individuals more liberty without providing the right environment to exercise control over their data.[38] A solution would be for PIMS settings to minimise data sharing by default without requiring the individual to take any important decisions at the initial stage of using a product or service. Any non-essential data processing decision should require an opt-in and active engagement of the user. All optional data processing should be turned off by default (Art. 25 GDPR), taking into consideration the intrinsic weaknesses of vulnerable persons and, at the same time, giving them control over their data if they wish to change those settings. The necessity to change them would inherently result in more informed choices.

Many smart devices do not communicate their privacy policies and users' data protection choices in a transparent way. For example, some IoT products do not have any user interface (particularly troublesome for vulnerable persons) and do not provide their users with an easy option to learn about or modify their privacy settings.[39] By managing all of their data on a single device (the PIMS), vulnerable people would not need to worry about choosing settings on all of their devices separately and they could benefit from a much more usable interface, with dashboards which visualise datasets in a more comprehensible manner.[40]

3.2 Protecting Vulnerable Subjects from Mishandling Other People's Data by Mistake

Issues regarding data control do not only concern the PIMS owner's personal data but also personal data of other people stored within the system. Art. 82(2) GDPR states that 'Any controller involved in processing shall be liable for the damage

[37] Anciaux and others (n 27).
[38] Anciaux and others (n 27).
[39] Galen Gruman, 'IoT Silliness: "Headless" devices without a UI' (*InfoWorld*, 13 January 2015) <https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html> accessed 1 November 2022.
[40] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22(2) Personal and Ubiquitous Computing 317.

caused by processing which infringes this Regulation'. An implication of this is that a vulnerable person might be liable for the damage caused by processing other people's personal data on their PIMS.

A PIMS can store personal data of various persons such as, for example, contact details of doctors gathered by a smart health product. In principle, PIMS should guarantee data's confidentiality on behalf of the vulnerable consumer. However, the case might be that the vulnerable consumer accesses personal data of other individuals through the system and decides to send it to untrusted third parties. Users of smart home devices may have lawful reasons to process others' personal data, including for a legitimate interest pursued by themselves,[41] whether for a domestic purpose or not.[42] Vulnerable users, however, are in a much weaker position to make the balancing decisions. For this reason, this paper considers that PIMS should block the possibility of undertaking certain actions with sensitive data. For example, vulnerable users should be capable of accessing the contact details of their doctors gathered by smart products and stored inside the PIMS but not be able to send this data to third parties. For some authors, such restrictions should be extended to all owners of PIMS and not only vulnerable individuals. They argue that consumers should not be given access to all of the PIMS content.[43] However, the question lies as to where exactly the line should be drawn between data that can be fully controlled and data for which certain actions should be prohibited. What kind of actions should individuals be able to undertake regarding other people's personal data stored on their PIMS? There is no easy answer to this question but designers and developers of the PIMS hardware and software should cooperate with lawyers to find the most GDPR compliant solutions. In general, this article considers that the answer should be the minimum amount of data possible without previously obtaining the consent of the data's true owner. In most cases, transferring other people's data should not be needed unless a person previously entered, for example, in a contractual agreement that requires such transfers in which case there will already be a lawful legal basis. Designers of PIMS systems have an important role in supporting data controllers to fulfil data protection duties,[44] and when it comes to vulnerable users of PIMS, additional caution should be made to minimise the risk of them accidentally 'commoditising' personal data of others.

3.3 Limiting Parents' and Legal Guardians' Data Management Powers

In a smart home, personal data will reside with the persons from whom the data has originated but control could be temporarily entrusted to a different individual (such as a parent or legal guardian) to handle, for example, a vulnerable adult's health

[41] GDPR, Art 6.1 (f).
[42] For a discussion on how smart homeowners might be held responsible as a data controller without being covered by the household exemption provided by art 2.2 (c) GDPR, see Chen and Urquhart (n 67).
[43] Anciaux and others (n 27).
[44] GDPR, Recital 78.

record gathered through a smart product.[45] As a consequence, vulnerable users of PIMS do not necessarily possess the privileges required to control their data stored inside the platform.[46] Parents might be in control when their child is underage, a legal guardian when adults are vulnerable or the system could be simply set up giving control to a specific person in the household. A PIMS can gather all of smart homes users' personal data and they need to be protected from each other's unintended (or intended) actions.

Some consider that parents are not best suited and should not be trusted to ensure their children's protection online, 'as many are unaware or unable to mediate their children's online activities'.[47] Parents do not always have the best answer nor possess the digital literacy skills needed to effectively manage their children's data. This leads to the question of whether consent is really informed when provided by them.[48] The same issue can be raised concerning legal guardians taking care of vulnerable adults.

Independently of legal guardians' and parents' capacity to make informed choices, another issue is their good intentions. While most of them will hopefully have the best interests of the vulnerable persons under their protection as the top priority, this will not necessarily be the case in every household. In June 2018, the New York Times published an article in which it warned against the increasing number of IoT products involved in domestic abuse cases.[49] For example, a woman in distress informed the hotline that code numbers to enter her home change every day and she does not understand why. This kind of power could also be used in relation to vulnerable people and their data. While domestic abuse may be a problem that is not easily solved by any kind of PET, some issues linked to the processing of vulnerable individuals' data for malicious purposes by other members of the household could be prevented and limited through the design of PIMS systems. Unless this is required by law (for example, for health-related reasons) or unless a vulnerable person has given informed consent (if this is possible depending on their condition), the legal guardian's or parents' power to process vulnerable people's data should be restricted.

---

[45] Andy Crabtree and Richard Mortier, 'Human Data Interaction: Historical Lessons from Social Studies and CSCW' (ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, Oslo, 2015).

[46] Anciaux and others (n 27).

[47] Sonia Livingstone and Leslie Haddon, 'EU Kids Online' (2009) <http://eprints.lse.ac.uk/24372/1/EU%20Kids%20Online%20final%20report%202009%28lsero%29.pdf> accessed 1 November 2022; Milkaite and Lievens (n 3) 295.

[48] Simone van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) 34(2) Wisconsin International Law Journal 409.

[49] Nellie Bowles, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' (*The New York Times*, 2018) <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> accessed 1 November 2022.

Another situation where the parent or legal guardian's decision on the personal data of a vulnerable subject could be made to the latter's detriment concerns the monetisation of such data. The approach of monetising data through cloud models is reflected in smart homes, 'with personal data collected by IoT devices typically being distributed to the cloud for processing and analytics'.[50] However, some researchers have recently noted that new payment mechanisms are appearing in relation to data and privacy related purchases, and this in context of edge-computing architectural models.[51] Indeed, 'making personal data available for access and trade is expected to become a part of the data driven digital economy'.[52] Trading data and creating value for all stakeholders will be important for the survival of PIMS as it could enable their more widespread adoption.

While temporarily allowing a third party to process data in exchange for rewards is arguably an acceptable practice under the GDPR provisions on data portability,[53] this should be done with caution as trading sensitive data could expose individuals' intimate details of their personal everyday life to unknown entities.[54] For example, if their smart health devices transfer data to third parties and those third parties do not have effective data protection mechanisms in place or sell this data to insurance companies (to establish consumer profiles), this could potentially negatively affect vulnerable persons. Both 'ordinary' data and metadata can contain a lot of information about a person and their habits. If a certain PIMS allows data monetisation, it should also contain mechanisms preventing monetisation by untrustworthy external organisations.

In any case, this article considers that legal guardians and parents should not be able to monetise data of the vulnerable people under their protection. The power they have to manage vulnerable individuals' data should not be used for their own benefit and at the expense of those they are supposed to protect. As it has been mentioned above, parents (or legal guardians) might not understand the intricacies of personal data processing and, even if they have good intentions, they may not be able to comprehend the consequences of selling their children's data to third parties. For this reason, monetising a vulnerable person's data should only be allowed, according to this paper, when vulnerable persons are capable of providing informed consent themselves.

In addition to the above-mentioned data management issues related to who has access to data and how they can control it, questions remain as to when confidentiality should be prioritised over control (or vice versa) from a design and

[50] Urquhart, Crabtree and Lodge (n 18).
[51] Wired, 'Decentralised AI has the Potential to Upend the Online Economy' (2021) <https://www.wired.co.uk/article/decentralised-artificial-intelligence> accessed 1 November 2022.
[52] Perera and others (n 30).
[53] GDPR, Art 20.
[54] Urquhart, Sailaja and McAuley (n 40).

legal perspective. The normative landscape is complicated by the special circumstances that vulnerable data subjects find themselves in. This may shake up the libertarian-paternalistic equilibrium in the regulatory debates on the extent to which privacy-management decisions should be left to individuals. A potential practical solution is offered in the next sections through edge-computing PIMS and the latter's impact on the confidentiality of vulnerable people's data in a smart home context is analysed. The practical security benefits of edge-computing PIMS are explored as well as how they support data minimisation.

4. Beyond Confidentiality: The Underlying Value Orientation of PIMS

4.1 The Current Focus on the Confidentiality Paradigm When Designing IoT Products

Gürses drew attention to the techno-centric nature of data protection and the focus on confidentiality adopted by many computer scientists.[55] Techno-centricity can be defined as an interest 'in understanding how technology leverages human action, taking a largely functional or instrumental approach that tends to assume unproblematically that technology is largely exogenous, homogenous, predictable, and stable, performing as intended and designed across time and place'.[56] It focuses on the effects of the technology while ignoring how it is linked to historical, cultural and social influences. This approach is opposite to human-centricity, which places the way in which people make sense of and use technology at the forefront. Human-centric approaches seem to reflect GDPR's focus on control (in addition to confidentiality) and its differentiation between vulnerable and other citizens. Human-centricity does take social, cultural and historical contexts into account but tends to minimise the role of technologies.[57] As Gürses stated, 'social practices in spaces subject to ubiquitous surveillance are constituted by existing surveillance practices, technologies and by PETs, whereas PETs are the product of humans, their own social practices and conceptions of how surveillance is made effective and can be countered'.[58] Privacy by design obligates manufacturers of IoT devices to embed all data protection principles from initial design stages.[59] When thinking about data protection by design, neither the confidentiality techno-centric nor the control human-centric approaches seem sufficient alone. Before delving deeper into this topic and analysing the control and confidentiality entanglement, it is necessary to respond to the question as to what this article means by privacy-as-confidentiality and privacy-as-control.

---

[55] Seda Gürses, 'PETs and their Users: a Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm' (2010) 3(3) Identity in the Information Society 539.
[56] Wanda J. Orlikowski, 'Sociomaterial Practices: Exploring Technology at Work' (2007) 28(9) Organization Studies 1435, 1437.
[57] Orlikowski (n 56).
[58] Gürses (n 55).
[59] Article 29 Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (WP 202, 2013).

Privacy-as-confidentiality strives to ensure that technologies support minimal information loss or leaks from persons using smart products. This is distinctive of PETs, whose researchers use mainly cryptographic methods to, for example, perform analysis on whole datasets while learning as little as possible about the persons within them.[60] Privacy-as-confidentiality is characterised by an environment full of adversaries who cannot be trusted. Researchers often consider that the main objective of privacy technologies is to respond to risks associated with untrusted environments. Privacy-as-control, on the other hand, tries to build trust between organisations that could otherwise be considered as adversaries, and turn them into 'responsible stewards, rather than ruthless exploiters, of data'.[61] It is the GDPR's approach, through which the regulation mandates data controllers to respect the rights of data subjects, such as the right of access or erasure of their data. In the context of smart devices used by vulnerable people, it is worth discussing whether achieving confidentiality is more important than promoting control.

An example of how these two paradigms might collide in the smart home context could be found in how Apple handled data subject requests. After an explicit application to obtain personal data recorded by the Siri voice assistant, Apple declined relying on the notion of privacy by design.[62] The company's choices are what some have presented as a 'rather narrow definition of privacy, which largely addresses confidentiality and data security'.[63] It is uncertain what has been the company's true rationale for limiting data subjects' rights and this should have been explained (for example, by publishing data protection impact assessments). However, taking into consideration GDPR's requirement to implement special data protection measures concerning children (Rec. 38 GDPR) and vulnerable people in general (Rec. 75 GDPR), Apple's decision to favour confidentiality could be justifiable. Of course, companies should strive to ensure that both confidentiality and other rights can be effectively exercised. Until such systems exist, for children or some vulnerable adults (in contrast to people that may be capable of ensuring both effective protection and control of their data), the advantages of exercising certain data rights (such as the right of access) will probably not be greater than those of true data confidentiality (if exercising those rights would mean more risks of data breaches). Data controllers should regularly re-evaluate their decisions in line with the 'state of the art' criteria that requires them to stay up to date with technological

[60] Vasilios Mavroudis and Michael Veale, 'Eavesdropping Whilst You're Shopping: Balancing Personalisation and Privacy in Connected Retail Spaces' (Proceedings of Living in the Internet of Things: Cybersecurity of the IoT, London, 2018) 4.
[61] Mavroudis and Veale (n 60).
[62] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8(2) International Data Privacy Law 105.
[63] Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24(2) International Journal of Law and Information Technology 151.

developments and how the latter can support the implementation of GDPR provisions.[64]

Confidentiality means that someone is protected from the observation of others while control is a model enabling the data subject. Theoretically, these two values of confidentiality and control do not need to be mutually exclusive. As Cohen stated back in 2000, 'the characterization of the data privacy problem as driven by technological trade-offs grossly oversimplifies the choices that we face' because 'architectures of data collection are chosen'.[65] And what is chosen can be changed. There is a possibility that an instrument could serve both purposes. Edge-computing PIMS might be such a solution. The security and control related benefits and issues of using PIMS by vulnerable individuals in smart homes will be discussed in the next sections.

4.2 The Security Benefits of Local Data Storage

The insecurity of smart homes is currently an important problem in the world and many essential security features are missing in smart devices (such as regular software updates or strong authentication measures).[66] Moreover, most IoT devices transfer users' data to the cloud, either for computation or storage. This article argues in favour of recognising the value of local data processing and edge-computing architectures, especially in the light of the importance of the integrity and confidentiality of vulnerable people's personal data. Edge-computing models are emerging in some degree as a response to the increased number of insecure smart devices and the associated growing amount of data collected by companies for data analysis purposes. This approach has advantages in terms of facilitating data protection compliance and security management in people's homes.[67] It prevents inherent security risks of data processing in the cloud. Ensuring vulnerable people's data is processed by IoT devices in a secure manner and at the edge would support

[64] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (12–13 November 2019) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf> accessed 1 November 2022.

[65] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52(5) Stanford Law Review 1373, 1436.

[66] Kayleen Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (2017) 17(2) Oxford University Commonwealth Law Journal 265; Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (Norton 2018); Scott R. Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93(1) Texas Law Review 85.

[67] EDPS, 'Opinion 9/2016 on Personal Information Management Systems' (20 October 2016) <https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en> accessed 1 November 2022; Jiahong Chen and Lachlan Urquhart, 'On the Principle of Accountability: Challenges for Smart Homes and Cybersecurity' in Andy Crabtree, Haddadi Hamed and Mortier Richard (eds), *Privacy by Design for the Internet of Things: Building Accountability and Security* (IET 2021).

companies' compliance efforts with GDPR's integrity and confidentiality principle, a prerequisite for lawful data processing.

In addition, another security benefit in the context of edge-computing architectures is that actuation does not depend on uninterrupted connection to the internet, which increases the system's resilience and reduces data processing costs.[68] For example, during an internet connection downtime, whether caused by a cyberattack or simply a technical failure, authentication for a smart lock may stop to function if it relies entirely on the cloud model.[69] This may not just cause the user to be locked out, which is particularly a problem if the user is a vulnerable person, but may also breach the security duty under Art. 32.1, especially regarding the availability and resilience requirements.

In 2015, Mattel produced a smart device called the Hello Barbie doll. This Wi-Fi enabled smart toy was presented as the first interactive doll ever created, capable of listening and having conversations with children. The doll had a microphone which recorded children and then sent those recordings to third parties for data processing. Matt Jakubowski, a security researcher working in the field of cybersecurity, was successful in quickly hacking the doll. This allowed him to access the system, acquire account data, files containing audio recordings and to use the toy's microphone itself.[70] Children could be the target of hackers for various reasons. They could be used to acquire sensitive information or their toy could be hacked to gain access into other smart devices in the smart home. In this scenario, the dangers concerning data transfers into the cloud for processing by unknown third parties could be reduced by using edge-computing PIMS. For example, referring again to the example of the Databox PIMS, the latter 'enables the data subject to control external access to data via app manifests that provide granular choice encoded as enforceable data processing policies on-the-box, and constrains data distribution to the results of processing'.[71] In addition, 'The IoT Databox stores data in a distributed array of containers, which encrypt data at rest'.[72]

Vulnerable adults, such as people living with dementia, are unfortunately often victims of cybercrimes.[73] Cybercriminals might hack into a smart device and obtain

---

[68] Andy Crabtree and others, 'Building Accountability into the Internet of Things: the IoT Databox Model' (2018) 4(1) Journal of Reliable Intelligent Environments 39.
[69] Richard Speed, 'Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb' (*The Register*, 17 May 2018) <https://www.theregister.co.uk/2018/05/17/nest_outage/> accessed 1 November 2022.
[70] Samuel Gibbs, 'Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children' (*The Guardian*, 26 November 2015) <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children> accessed 1 November 2022.
[71] Urquhart, Crabtree and Lodge (n 18).
[72] Urquhart, Crabtree and Lodge (n 18).
[73] Financial Times, 'Living with the Cost of Dementia' (2021) <https://www.ft.com/content/4baeeb4e-d680-11e6-944b-e7eb37a6aa8e> accessed 1 November 2022.

personal data themselves or contact their target through a smart product. Edge-based PIMS could help in such circumstances by detecting unusual activities and informing the relevant person or institution. For example, a vulnerable adult or the legal guardian could download a bank's fraud detection app. The bank would contact the app in the case of unusual activity. The user's precise location would not be disclosed but only information on whether they are located where the unusual activity is taking place.[74] The bank would then be able to prevent fraud and protect vulnerable individuals, the most frequent victims of these kinds of criminal activities. All of this would happen in a privacy-preserving way in which only the data necessary to answer a particular query (is the data subject located where the unusual activity is taking place?) would be transferred to the third party asking for information. Such an app can be installed on the PIMS and integrated with all of the data traffic coming from vulnerable people's smart devices.

4.3 Minimising Data Processing Risks by Answering Only Specific Queries

PIMS can help comply with the data minimisation principle (Art. 5.1 (c) GDPR). Some authors explain that in line with this principle smart devices should reduce the amount of data transferred from smart products by changing raw data into aggregated data and deleting the former as soon as the data necessary for processing has left the device.[75] This is precisely what certain PIMS do as they take 'computing to the data, rather than data to the computing as per the current 'cloud' paradigm, and this has distinct computational as well as social advantages'.[76] Among others, it removes the necessity for international data transfers to remote servers in third countries (thereby reducing data processing).

An example of how PIMS could be useful in the specific context of vulnerable individuals is when smart devices try to obtain information on users' age or consent from their legal guardian.[77] Even though there is no explicit provision in the GDPR that mandates data controllers to ask about data subjects' age, this is still necessary, as processing on the basis of consent obtained from an underage child would be unlawful. This needs to be done in conformity with the data minimisation principle, enshrined in Art. 5.1 (c) GDPR. One benefit of PIMS in this context is that all smart home devices would receive the relevant information (about the legal guardian or data subject's age) from the PIMS, without the necessity for each device to ask the same questions. Moreover, this information would be collected at the edge, without the need to worry about excessive data collection by data controllers. Only the required information (confirmed age or identity) would be transferred to the relevant third party.

[74] Alan Chamberlain and others, 'Special Theme on Privacy and the Internet of Things' (2018) 22(2) Personal and Ubiquitous Computing 289.
[75] Crabtree and others (n 68).
[76] Chamberlain and others (n 74).
[77] Milkaite and Lievens (n 3).

In terms of how this could be achieved, this is more of a question of how to do it effectively and in a privacy-preserving manner, as in terms of security, vulnerable people's data would be kept on the PIMS itself. However, this is also crucial for vulnerable people's data protection rights. If the identification of a vulnerable person or their legal guardian is made difficult, they will not be able to easily exercise their rights in a safe manner. Firstly, PIMS would need to be able to contain information on who is a person's legal guardian or who is a child's parent. To obtain such information, the PIMS could, for example, make a request to a governmental database. However, this request should not divulge unnecessary data to third parties and only information that a request has been made should be transferred.

In certain cases, a data subject's identification could be also facilitated through the use of biometrics. However, in Europe, biometrics seem to be often associated by citizens with privacy invasive technologies. This could be changing (or not) with the appearance of new phones and other devices using such means to identify their owners. If the costs are not prohibitive, and biometric identification can be done on the edge, in a privacy-friendly way, then it could be a more effective solution. For example, facial recognition could recognise whether the user is a child. This would facilitate further actions within the PIMS as the system would know that the user is underage. In the case of children, biometrics would have the added benefit of simplifying the process as connecting to a database to confirm whether the user's response is correct would no longer be necessary. Of course, data controllers could just trust data subjects' responses without further verification, but it would be naïve to think that those responses would always be truthful.

The local storage of raw data and minimised transmission of aggregated data may in some cases happen at the cost of a degree of utility or efficiency, which can be seen by some as suboptimal in realising the full potential of smart technologies. However, both of these features of edge-based PIMS align strongly with the confidentiality paradigm and, as discussed, when it comes to the use of vulnerable people's data, the balance between confidentiality and control should tilt more towards the former (if both cannot be achieved at the same level).

5. Conclusion

Technologies have an undeniable impact on how people behave in the online world and, as a consequence, on what they can and cannot do with their data. A set of technical approaches have emerged under the name of privacy enhancing technologies to promote safer and more effective processing of personal data. PIMS are one type of such technologies, with the particularity that they strive to offer a full solution to GDPR compliance requirements. This article has focused on edge-computing PIMS. While relying on the cloud was historically justifiable, current technological developments permit edge-computing systems to offer the same benefits as cloud-based systems. Both architectures can offer efficient computing utility or storage, virtualisation and access to services through networking, while edge-computing has the added security benefit of processing data locally. There is a

certain momentum that needs to be recognised in favour of decentralised data processing. The issue with edge systems is their current lack of widespread adoption. There must be incentives – such as governments leading through example by adopting those systems within their structures, or new ways of monetising data gathered at the edge – that will convince organisations to use and implement edge-computing PIMS.

PIMS can empower users while switching off all unnecessary data sharing settings by default. The fact that such systems enable the management of various smart devices at the same time through a single transparent interface could facilitate vulnerable people's or legal guardians' potential decisions to opt-in to data processing. PIMS can store personal data of several persons. For this reason, this article argues in favour of restricting what a vulnerable person can do with other people's data stored within a PIMS to the minimum legally required (for example, accessing contact details of a doctor), unless consent has been previously obtained. Similarly, parents' and legal guardians' data management powers should also be limited through the PIMS design. Some argue that parents are not the best suited and should not be entrusted to ensure their children's data protection online. Moreover, legal guardians could misuse data of the persons they are supposed to protect. For this reason, reducing their data management powers seems like the more responsible approach. This raises the technical issue of how PIMS systems will know which data can be accessed and processed by a legal guardian. Finally, while PIMS should offer possibilities of data monetisation to promote their widespread adoption, legal guardians should not be allowed to monetise data of vulnerable people as even if they have good intentions; they might not be able to predict the negative consequences that such monetisation could cause. Only if a vulnerable individual is capable of providing consent should their data monetisation be allowed through PIMS systems.

In terms of data protection by design, current privacy enhancing technologies seem to focus on privacy-as-confidentiality as opposed to privacy-as-control. Some authors have criticised this approach as it impedes data subjects' capacity to exercise their rights and to manage data risks themselves. If a company does limit the possibility to exercise certain data protection rights, it should certainly justify this (for example, through data protection impact assessments). However, this article considers that if an organisation is transparent about its privacy by design measures and their implications, and if a compromise needs to be made, prioritising privacy-as-confidentiality could be the right solution in the context of vulnerable individuals using smart products. The confidentiality of their personal information will be probably more important that the exercise of certain GDPR rights (such as the right of access). A solution to this inherent tension between privacy-as-confidentiality and privacy-as-control could be edge-computing PIMS, as they can offer both enhanced confidentiality and increased data control. From a security perspective, processing data locally signifies that raw data is stored at the network's edge, which prevents the risks intrinsic to cloud data computations. Only data necessary to respond to particular queries is sent to third parties. Moreover, in the

case of edge architectures, functioning does not rely on uninterrupted connectivity, which increases a smart home's resilience and the protection of vulnerable citizens. In addition, edge-computing PIMS detect unusual activities and data processing based on unusual data requests will not take place unless user's consent is obtained. The fact that data is processed at the edge also facilitates compliance with the data minimisation principle. When obtaining information on users' age or identity (for example, to establish whether a particular person is a legal guardian), the problem of potential excessive data collection by data controllers would disappear, as PIMS would transmit only the required information (confirmed age or identity) to the relevant third party.

In general, this study considers that there is a true opportunity with edge-computing PIMS to reconcile privacy-as-confidentiality and privacy-as-control within a system that allows both to co-exist in a more harmonious manner. The increased data security, data minimisation and data protection by design and by default that processing at the edge enables can greatly support companies in meeting their GDPR obligations. A widespread adoption of PIMS could facilitate GDPR compliance and increase the protection of vulnerable people's data and rights. Further interdisciplinary research is needed to determine how precisely this can be implemented in practice, but it is of paramount importance to first establish what kind of privacy we should strive for in personal information management systems.