COMPUTER LAW & SECURITY REVIEW 34 (2018) 1039–1052

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Ownership of personal data in the Internet of Things

Václav Janeček[a,b,c,d,*]

[a] *Oxford Internet Institute, University of Oxford, Oxford, United Kingdom*
[b] *Faculty of Law, University of Oxford, Oxford, United Kingdom*
[c] *St Edmund Hall, Oxford, United Kingdom*
[d] *Faculty of Law, Charles University, Prague, Czech Republic*

ARTICLE INFO

Article history:

Keywords:
Personal data
Personal information
Non-personal data
Data
Information
Ownership
Internet of Things
EU law
Property
GDPR
Review

ABSTRACT

This article analyses, defines, and refines the concepts of ownership and personal data to explore their compatibility in the context of EU law. It critically examines the traditional dividing line between personal and non-personal data and argues for a strict conceptual separation of personal data from personal information. The article also considers whether, and to what extent, the concept of ownership can be applied to personal data in the context of the Internet of Things (IoT). This consideration is framed around two main approaches shaping all ownership theories: a bottom-up and top-down approach. Via these dual lenses, the article reviews existing debates relating to four elements supporting introduction of ownership of personal data, namely the elements of control, protection, valuation, and allocation of personal data. It then explores the explanatory advantages and disadvantages of the two approaches in relation to each of these elements as well as to ownership of personal data in IoT at large. Lastly, this article outlines a revised approach to ownership of personal data in IoT that may serve as a blueprint for future work in this area and inform regulatory and policy debates.

1. Introduction

Internet of Things (IoT) technologies are becoming increasingly more pervasive. Within the EU28 alone, the estimated number of connected 'things' was 1.8 billion in 2013 and is expected to reach 6 billion by 2020.[1] These so-called 'smart' devices will foster our interactions with the environment by facilitating transport and logistics, for example, as well as delivery of services like healthcare and security. At the same time, IoT devices generate and collect a wealth of personal data, whose management poses serious ethical[2] and

* Corresponding author at: St Edmund Hall, Queen's Lane, OX1 4AR Oxford, United Kingdom.
E-mail address: vaclav.janecek@law.ox.ac.uk

[1] S Aguzzi and others, *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination* (European Commission 2014) 10, 26, 61. Globally, the number of connected devices is expected to grow from 9 billion in 2013 up to 50 billion by 2020: OECD, *OECD Digital Economy Outlook 2017* (OECD Publishing 2017) 247; GAO, *Technology assessment: Internet of Things: Status and implication of an increasingly connected world* (GAO-17-75, May 2017) 1; McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (McKinsey 2015) 17.

[2] J Van den Hoven, *Internet of Things Factsheet Ethics* (European Commission 2013).

https://doi.org/10.1016/j.clsr.2018.04.007
0267-3649/

legal[3] questions. Ownership of personal data underpins the issues revolving around data management and control, such as privacy, trust,[4] and security, and it has also important implications for the future of the 'digital' economy and trade in data.[5] This is why debates on introducing the concept of data ownership as a legal right have recently emerged at the EU level[6] and beyond,[7] and why they are still thriving, although the majority of the legal doctrine and now also the European Commission have reservations about the data ownership concept.

Due to legal developments in personal data protection, starting with the fundamental right to respect for private life,[8] over the fundamental right to protection of personal data,[9] and recently culminating by the data subject's rights granted by the General Data Protection Regulation (GDPR),[10] it became impossible to think of any data ownership without also thinking about ownership of *personal* data. The problem is, however, that the line between personal and non-personal data is a moving target and data that are now seen as non-personal data may become (thanks to analytical and technological advancements) personal data in the future.[11] Thus, exploring the conceptual limits of ownership of personal data must precede debates on ownership of purely non-personal data (e.g. data employed in smart farming).[12] In fact, personal data have already been recognized as one of the key economic assets,[13] and avoiding questions regarding their ownership is thus problematic even in the light of these economic trends. Moreover, the need for the analysis stems from the nature of the IoT world in which many of us already live. Take, for instance, 'smart cities' where big data companies may soon be able to privatize data (including personal data), despite them being largely collected without prior consent of data subjects.[14] In response to these challenges, a number of ownership-like types of technological solution are also emerging. One such example is the AURA platform—a Personal In-

[3] See J Drexl and others, 'Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate' (2016) *Max Planck Institute for Innovation & Competition Research Paper No 16-10* <https://ssrn.com/abstract=2833165⟩ accessed 16 November 2017.

[4] M Taddeo, 'Trusting Digital Technologies Correctly' (2017) 27 Minds & Machines 565; M Taddeo, 'Trust in Technology: A Distinctive and a Problematic Relation' (2010) 23 Know Tech Pol 283.

[5] See, e.g., TJ Farkas, 'Data Created by the Internet of Things: The New Gold without Ownership' (2017) 23 Rev Prop Inmaterial 5, 14; C Bartolini, C Santos and C Ullrich, 'Property and the cloud' (2018) 34 CLSRev 358; V Gazis and others, 'Short Paper: IoT: Challenges, projects, architectures' (2015) 18 International Conference on Intelligence in Next Generation Networks 145; A Whitmore, A Agarwal and L Da Xu, 'The Internet of Things—A survey of topics and trends' (2015) 17 Inf Syst Front 261, 266; IERC – European Research Cluster on the Internet of Things, *Internet of Things: IoT governance, privacy and security issues* (European Commission 2015) 10, 78–79.

[6] See, e.g., Commission, 'Building a European Data Economy' (Communication) COM (2017) 9 final, 9–10, 13; Commission, 'On the free flow of data and emerging issues of the European data economy, accompanying COM (2017) 9 final' (Commission Staff Working Document) SWD (2017) 2 final, esp. 23, 33–38; Osborne Clarke LLP, *Legal study on ownership and access to data* (European Commission 2016) <https://bookshop.europa.eu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/⟩ [https://perma.cc/82D8-9787]; N Duch-Brown, B Martens and F Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data' (JRC Digital Economy Working Paper 2017-01, European Commission 2017) 12ff <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf⟩ [https://perma.cc/NUM8-HVWB]; A Gärtner and K Brimsted, 'Let's talk about data ownership' (2017) 39 EIPR 461; S van Erp, 'Ownership of Data: The Numerus Clausus of Legal Objects' (2017) 6 Brigham-Kanner Property Rights Conference Journal 235; S Lohsse, R Schulze and D Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos/Hart Publishing 2017); F Thouvenin, RH Weber and A Früh, 'Data ownership: Taking stock and mapping the issues' in M Dehmer and F Emmert-Streib (eds), *Frontiers in Data Science* (CRC Press 2018). Thanks is due to Stephen Saxby for bringing my attention to the 2018 publication.

[7] Globally, see, e.g., IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (version 2)* (IEEE 2017) 141–42, 237–38, 247 [https://perma.cc/W5MT-VK9K]; McKinsey Global Institute (n 1) 11, 26, 104, 106, 107 and 113. For India, see Telecom Regulatory Authority of India, *Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector* (TRAI Consultation No 09/2017) 2 and 6 [https://perma.cc/ES29-ZVA4]. Thanks is due to Ashok Rajagopalan for bringing my attention to this Indian document. For Australia, see Productivity Commission, *Data Availability and Use* (Report No 82, 2017) 53, 65, 66, 177, 191, 196, 241 and 584 [https://perma.cc/6RKE-PCGL]. For China, see Arts 45 and 48 of the First Draft E-Commerce Law of the People's Republic of China (published 27 December 2016). Thanks is due to Vicky Cheng for bringing my attention to this Chinese document. For the USA, see Osborne Clarke LLP (n 6) 78–81. For the United Kingdom (if seen as a potential non-EU member), see <http://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notices/house-of-lords-media-notices-2017/october-2017/who-should-own-your-data/⟩ [https://perma.cc/73JB-8QJU].

[8] Art 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950.

[9] Art 8 of the Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

[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) (OJ L 119/2016).

[11] C Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Lohsse, Schulze and Staudenmayer (eds) (n 6) 332.

[12] See S Wolfert and others, 'Big Data in Smart Farming – A review' (2017) 153 Agricultural Systems 69; J Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 JIPITEC 257. cf also Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' COM (2017) 495 final; Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final.

[13] World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (Geneva 2011) <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf⟩ [https://perma.cc/T7JL-BZXK].

[14] See L Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 EDPLR 28, 29, 33–34.

formation Management system (PIM)[15]—which was recently introduced by Telefónica in Spain and which, in contrast with trends in the smart cities, allows end-users to control relevant data that their mobile operator holds about them (e.g. the user's geolocation) and to decide with whom these data will be shared.[16]

In this article, I analyse, define, and refine the concepts of ownership and personal data to bring existing debates about ownership of personal data to common ground (Section 2). Then, I review theories of ownership and reasons supporting ownership of personal data to consider whether, and to what extent, the concept of ownership can be applied to personal data in IoT. My analysis is framed around two main approaches shaping all ownership theories: a bottom-up and top-down approach. I contrast these two approaches by looking at whether stabile ownership is yet to be created by positive law (the top-down approach) or whether positive law is meant to stabilize already existing, though instable, *de facto* ownership (the bottom-up approach). Via these dual lenses, I review reasons explaining and justifying propertisation of personal data in IoT as well as reasons supporting to whom these data should belong. My aim is to unveil the advantages and disadvantages of the two approaches and to frame the existing debates (Section 3). To show potential directions for consistent and sustainable policies and law-making in this regard, I outline a revised approach to ownership of personal data that may serve as a blueprint for developing this intellectual structure, should it be introduced in the first place (Section 4). Finally, I conclude that—in the context of the EU law—either a revised bottom-up approached ownership theory is needed or data ownership initiatives are to be, at least partially, repealed (Section 5).

Lastly, a terminological point needs to be made. In this article, I use the phrase 'ownership of personal data', because the expression 'personal data ownership', albeit stylistically more elegant, invites unclear and biased thinking by signalling that the *personal* data should be owned *personally* by the data subject. The desired allocation of ownership, however, is yet to be explored in this paper.

2. The concepts of ownership and personal data in the context of European law

2.1. *Ownership*

Since the concept of ownership is not defined at the EU-law level,[17] and since national legal systems define ownership differently, I first conceptually canvass a minimal definition of ownership. From a comparative viewpoint, a main distinction can be drawn between the civil law and common law understanding of ownership.[18] The civil law recognizes a limited number of property rights and a limited number of legal objects that can be subjected to these property rights (the so-called *numerus clausus*).[19] In contrast, the common law is more flexible and allows private parties more freedom in the types of ownership interests which they can create.[20] Therefore, the civilian idea of ownership is an absolute dominion encompassing all the listed rights (*numerus clausus*) over the relevant object; whereas in the common law tradition, ownership includes a variety of different rights over the same property. In common law, therefore, ownership can be gradual: you can have more or less ownership depending on how large the bundle of your property rights in the object is. To overcome this civil law/common law divide and to avoid conceptual issues stemming from the debate about the nature of ownership,[21] I refer to ownership as to a full-ownership, i.e. a bundle of all property rights. Such working definition can be acceptable in both legal traditions.

The second important comparative observation is that the civil law considers ownership an absolute right *erga omnes*, i.e. a right that gives rise to legal protection of property against everyone, whereas common law recognizes personal property rights (*in personam*) and real property rights (*in rem*) of which only the latter are exigible against the entire world.[22] This is why common lawyers can conceive of ownership of personal data as giving the owner a legal protection both relative to a particular person (ownership rights *in personam*) and absolutely against everyone (ownership rights *in rem*).[23] To clear the ground for analysing ownership of personal data in IoT in Europe, I proceed with an absolute concept of ownership to accent the common *erga omnes/in rem* feature of ownership

[15] European Data Protection Supervisor, 'EDPS Opinion on Personal Information Management Systems' (Opinion No 9/2016) <https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf> [https://perma.cc/X236-GR48].

[16] Telefónica, 'Telefónica presents AURA, a pioneering way in the industry to interact with customers based on cognitive intelligence' (press release, 26 February 2017) <https://www.telefonica.com/en/web/press-office/-/telefonica-presents-aura-a-pioneering-way-in-the-industry-to-interact-with-customers-based-on-cognitive-intelligence> [https://perma.cc/F59Q-LV74]. In 2018, the platform shall be launched also in Germany, the UK, Brazil, Argentina and Chile, possibly expanding to 11 markets by 2020 (Telefonica to launch Aura AI platform in 6 markets in February (telecomaper news, 30 November 2017) <https://www.telecompaper.com/news/telefonica-to-launch-aura-ai-platform-in-6-markets-in-february–1222638> [https://perma.cc/EES2-YM2M]).

[17] See more in S van Erp and B Akkermans, 'European Union property law' in C Twigg-Flesner (ed), *The Cambridge Companion to European Union Private Law* (CUP 2010) 173.

[18] See U Mattei, *Basic Principles of Property Law: A Comparative Legal and Economic Introduction* (Greenwood Press 2000) ch 1; M Graziadei, 'The structure of property ownership and the common law/civil law divide' in G Michele and S Lionel (eds), *Comparative Property Law: Global Perspectives* (Edward Elgar Publishing 2017).

[19] van Erp (n 6) 235; B Akkermans, *The Principle of Numerus Clausus in European Property Law* (Intersentia 2008); J Gordley, *Foundations of Private Law: Property, Tort, Contract, Unjust Enrichment* (OUP 2006) 49.

[20] Gordley (n 19) 49; van Erp (n 6) 236.

[21] A Ross, 'Tû-Tû' (1957) 70 HarvLRev 812; JR Pennock and JW Chapman, *Property* (New York UP 1980). More recently, e.g., J Waldron, '"To Bestow Stability upon Possession" – Hume's Alternative to Locke' in J Penner and HE Smith (eds), *Philosophical Foundations of Property Law* (OUP 2013).

[22] Gordley (n 19) 49; Mattei (n 18) 8–9.

[23] C Rees, 'Who owns our data?' (2014) 30 CLSRev 75, 77–78.

in both main European legal traditions. Besides, the European Commission used the same understanding of ownership with regard to data in its communication from 2017,[24] which further justifies my restrictive interpretation of the term.

Conceptually, then, ownership entails four elements that jointly answer the 'Who owns what?' question—an element of control, protection, valuation, and allocation of a resource. Let me explain this idea. Ownership rights have an active and passive aspect, giving the owner full-blown active control or full-blown passive protection of the resource. These active and passive rights relate to a valuable object, i.e. an object that is worth controlling and protecting. Thus, when the law guarantees a full-blown *erga omnes/in rem* control and protection over a valuable resource, we can speak of propertisation of the resource—the resource turns into property. Subsequently, it becomes necessary to allocate such property to someone. In Section 3, I analyse all four elements to explore why the law should allow someone to control and protect personal data, and to whom these valuable data should be allocated.

2.2. *Personal data*

Personal data are now legally defined in Article 4(1) of the GDPR as follows:

> '[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject') […].

This definition illustrates the slippery language regarding personal data. On one hand, the GDPR, Recital 68 explicitly wants to 'strengthen the [natural person's] control over his or her *own data*' (emphasis added), thereby making a step towards 'data subjects' default *ownership of their personal data*'.[25] On the other hand, personal data are also referred to in the GDPR as '*personal information*'[26] or simply as '*information*'[27] relating to a natural person. This understanding, however, overlooks the conceptual distinction between data and information and has crucial implications when it comes to ownership of personal *data* as opposed to ownership of personal *information*.

Data and information are two distinct concepts. Imagine a stone containing Egyptian hieroglyphs. Until the discovery of the Rosetta Stone, the very same piece of writing would represent all the data, but convey no meaningful information to its reader.[28] Data can be defined as 'putative fact[s] regarding some difference or lack of uniformity within some context'.[29] In the given scenario, data are represented by the hieroglyphs and as such they are the source of information, depending on how we interpret them. There is thus no data-less information. This means that we need not to understand the information that any data may convey in order to treat the data as an asset from which valuable information may be extracted in the future.

In debates on data ownership, however, a clear conceptual distinction between data and information is missing.[30] The legal debates build on a related yet conceptually very distinct differentiation between the form (usually digital form) in which information is embodied and the meaning contained in that form (information itself). This difference has recently been described as a distinction between the syntactic level of information (the form) and the semantic level of information (the meaning).[31] For the purposes of discussing *data* ownership, this approach cannot bring the desired level of clarity, though, because it confuses *syntactic information* with *data*.

The confusion between the syntactic level of information (as a formal representation of information) and the data (as a source of identical information) originates from an information-centred starting point of these legal debates. The original question featuring in said debates was 'When *information* (not data) can be protected by the law?' and the answer was that while semantic information (i.e. information *per se*) can never be protected by the law because it would violate free access to information,[32] syntactic information can be given legal protection.[33] From the information-centred viewpoint this answer was satisfactory. Saying that syntactic information or more precisely the formal expression of information, for example in form of a digital sequence of data, can be legally protected addressed the relevant information-centred problem. The data-centred discourse, however, cannot make efficient use of this conceptual scheme, because its original questions are 'How can we protect *data*?' and 'What information can be extracted from *data*?', not 'How can we express some *information* in form of (e.g. digital) data?'.

The fact that the same data can be analysed in indefinite ways also gave rise to the concern that data collected in IoT environments may eventually reveal sensible personal information. Some argue that the same piece of data can be interpreted as substantiating both personal and non-personal information depending on the context and purpose of its use,

[24] Commission, 'On the free flow of data …' (n 6) 33.

[25] Recital 68 of the GDPR (emphasis added). See also Recital 7 of the GDPR.

[26] Recital 6 of the GDPR (emphasis added).

[27] Art 4(1) of the GDPR (emphasis added). See also Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (WP 136, 20 June 2007).

[28] This example is taken from L Floridi, 'Is Semantic Information Meaningful Data?' (2005) 70 Philosophy and Phenomenological Research 351, 359.

[29] L Floridi, 'Semantic Conceptions of Information', *The Stanford Encyclopedia of Philosophy* (Spring edn, 2017) <https://plato.stanford.edu/archives/spr2017/entries/information-semantic/> accessed 15 November 2017.

[30] See, e.g., G Malgieri, 'Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data' (2016) 4 Privacy in Germany 133; N Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence' in S Gutwirth and others (eds), *Computers, Privacy and Data Protection: An Element of Choice* (Springer Netherlands 2011) 39; N Purtova, 'Property rights in personal data: Learning from the American discourse' (2009) 25 CLSRev 507, 507; N Purtova, *Property Rights in Personal Data: A European Perspective* (Wolters Kluwer Law & Business 2012) 129; Gärtner and Brimsted (n 6) 464; Rees (n 23); van Erp (n 6) 247, 251; A De Franceschi and M Lehmann, 'Data as Tradeable Commodity and New Measures for their Protection' (2015) 1 Italian LJ 51, 51–52.

[31] Commission, 'On the free flow of data …' (n 6) 34; Lohsse, Schulze and Staudenmayer (eds) (n 6); H Zech, 'Information as Property' (2015) 6 JIPITEC 192; Thouvenin, Weber and Früh (n 6) 120–21.

[32] van Erp (n 7) 244; De Franceschi and Lehmann (n 30) 66.

[33] Commission, 'On the free flow of data …' (n 6) 34; Zech (n 31).

which leads to erosion of the line between personal and non-personal data.[34] Privacy advocates would therefore argue that since control over any data implies risk of control over personal information (not vice versa), it would be practically impossible to enforce informational privacy if someone could control any data by owning them exclusively.[35] This reasoning can quickly lead to quite radical conclusions—no exclusive data control, no data ownership, no trade in data. The property and market advocates, in contrast, would want to utilize the data and therefore secure stabile control over them. In their perspective, all massively collected data in IoT environments (except for the special class of data that are collected and identified as personal data from the outset) can be controlled, owned, and traded by anyone in principle.

The root of this problem is that EU law defines personal data reversely: data are the source of information which, if personal, reversely implies that the original data are also personal. This definition leads into a seemingly paradoxical situation in which no data are personal from the outset and all data can become personal from the outset. The clash between privacy and property advocated then looks like a chicken/egg problem in which it is unclear which of the two comes first: information-centred privacy arguments prioritize the personal chicken; data-centred property arguments are on the side of the data egg. However, the problem of personal information and data is a different one. The trick is that an egg made of data does not need to reveal or contain the chicken's personal information in every single case and can still can be considered valuable and worth protecting. We may value the egg at different levels of abstraction than is the level of personal information. For example, the egg contains precious albumen as well as information about resistant constructions—you may try to crack it in your fist yourself. Data and information simply cannot be compared with each other at the same level of analysis because they are fundamentally different categories. On this account, it is clear that personal and non-personal data are not conceptually incompatible categories.

To reconcile both views, i.e. to allow personal-information-centred privacy as well personal-data-centred control, we need to restrict the scope of the potentially so controlled personal data from an opposite direction. The key question must be whether some data contain personal information intrinsically and therefore *cannot* be defined as non-personal data from the outset. Examples of such data can be seen in the jurisprudence of the European Court of Human Rights (ECtHR). According to the ECtHR, a human DNA sequence or human cellular samples[36] 'contain substantial amounts of unique personal data'[37] and merely retaining them invades, without further justification, the fundamental human right to privacy under Article 8 of the European Convention on Human Rights from 1950. The reason why even the least form of control over these data (e.g. their retention) constitutes breach of personality rights is that, given the current state of knowledge, there is no meaningful interpretation of these data, according to which they do not objectively allow us to identify the individual data subject. These unique personal data contain 'intrinsically private information'[38] and controlling them is therefore almost like controlling one's individual identity. To use the chicken/egg analogy, these data reveal the chicken's personal information in every case. Thus, such intrinsically personal data must be excluded from our definition of personal data for the purposes of ownership issues, albeit they represent the core type of personal data as defined by the GDPR (note that the GDPR defines 'personal data' in Article 4 exclusively for the purposes of that regulation).

The main argument for excluding the intrinsically personal data from the scope of debates about data ownership combines conceptual, ethical, as well as legal aspects. One may argue that, from an ontological point of view, such data are constitutive of one's own identity, because 'there is no difference between one's informational sphere [construed by these intrinsically personal data] and one's personal identity'.[39] Ownership of such data would thus conceptually imply ownership of people's identities and the owner of the intrinsically personal data cannot exclude the individual's demands on these data unless he/she neglects the individual's identity in the first place. Consequently, ownership-like exclusive control of such data would be analogical to slave-holding or human trafficking, which is ethically problematic.[40] Any claim on these data would equal the Shylock's claim to cut off and take a pound of flesh from Antonio's body in return for his debt and that is not only ethically unacceptable but, in the light of fundamental human rights protection, also illegal.

Still, there remains a concept of personal data that is compatible with the concept of ownership, because not all personal data are intrinsically personal. Some personal data can be objects of our transactions just like a pound of sugar, or a barrel of oil because they do not need to contain personal information by default, i.e. intrinsically. A good example might be GPS data, your IP address, or data held in your personal task manager. For instance, the Federal Court of Australia recently confirmed that IP address is primarily made of metadata and that metadata are not (by default) subjected to privacy protection.[41] Although the same approach has not yet been explic-

[34] See Commission, 'On the free flow of data …' (n 6) 34; Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' COM (2017) 495 final; Osborne Clarke LLP (n 6) 41; N Purtova, 'Do property rights in personal data make sense after the Big Data turn? Individual control and transparency' (2017) *Tilburg Law School Research Paper No 2017/21*, 13–17 <https://ssrn.com/abstract=3070228> accessed 11 December 2017.

[35] Purtova (n 34) 13–17.

[36] *Aycaguer v France* App no 8806/12 (ECtHR, 22 June 2017), (2017) EHRLR 519; *S v United Kingdom* (2009) 48 EHRR 50 (ECtHR).

[37] *S v United Kingdom* (n 36) [75].

[38] ibid [104].

[39] L Floridi, 'The Ontological Interpretation of Informational Privacy' (2005) 7 Ethics Inf Technol 185, 195.

[40] See ibid 196; LM Katz, 'Philosophy of Property Law, Three Ways' in *Cambridge Companion to Law and Philosophy* (CUP 2018) 5 <https://ssrn.com/abstract=3076251> accessed 8 December 2017 (forthcoming); European Data Protection Supervisor Ethics Advisory Group (EDPS EAG), *Report 2018: Towards a digital ethics* (EDPS 2018) 24–25 <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> [https://perma.cc/XPQ7-43UK].

[41] *Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 [44], [73].

itly taken in the EU law,[42] we can argue that metadata concerning a data subject (e.g. the IP address or the length of a DNA sequence) are personal only extrinsically and therefore do not face the same conceptual, ethical, and legal issues as the opposing category. I will leave it to my readers to work out for themselves the correctness of these claims in relation to derivative data and operational data (which are, next to primary data and metadata, also considered distinctive categories of data).[43]

For the purposes of discussing data ownership, I therefore use the expression 'personal data' as a synonym for 'extrinsically personal data' and I contrast them with 'intrinsically personal data'. This revised definition (which contrasts extrinsically personal data with intrinsically personal data) fundamentally departs from the traditional contrast between personal and non-personal data. Yet since, I analyse *ownership* of personal data and not protection of personal data *privacy*, such revision and refinement are perfectly compatible with the understanding of personal data in the GDPR. Outside the GDPR, personal data do not need to be defined reversely as data about which we already know that they contain personal information.

3. Two approaches to ownership of personal data in IoT

3.1. *The top down and the bottom-up approach*

Modern theories explaining and justifying the origin of ownership, i.e. theories answering the question '*Why* the law should allow someone to own something?', follow either a top-down approach, sometimes referred to as the positivist approach to ownership, or a bottom-up approach, sometimes referred to as the natural law approach to ownership.[44]

In the top-down approach, some superior authority must posit ownership, otherwise it would not exist. *De jure* ownership thus precedes *de facto* ownership. It explains and justifies introduction of ownership by some authoritative reasons and goals, i.e. by reference to interests that are considered sufficient regardless of individuals' interests. It is important to stress though that these authoritative and, in democratic societies, public interests can be perfectly in line with individual persons' preferences—which may be a source of confusion when identifying the top-down approach to ownership of personal data—but that these individual non-authoritative interests are irrelevant.

By contrast, the idea common to all bottom-up approaches to ownership is that property rights, the owner and the valuable resource are all inherently pre-positive and would exist regardless the official legal system. In the bottom-up perspective, *de facto* ownership precedes *de jure* ownership, and the overarching reason why it is desirable to introduce *de jure* ownership is merely to bestow stability upon the *de facto* state of affairs. The core distinction thus is that whereas in the top-down approach the law posits and creates ownership as a fundamentally legal institute, i.e. something that would not exist without the positive laws; in the bottom-up approach the law protects and sustains ownership as a fundamentally pre-positive institute.

3.2. *Four elements supporting ownership*

Both the top-down and the bottom-up approach must encompass four elements supporting ownership of a resource—the elements of control, protection, valuation, and allocation of a given resource. To explain and justify why ownership of personal data should be introduced, we thus need to ask why we want to create someone's stabile *de facto* control and protection of valuable personal data (by introducing *de jure* ownership in the top-down approach); or whether someone already has *de facto* ability to control and protect valuable personal data, i.e. an ability upon which the law shall bestow stability (by introducing *de jure* ownership in the bottom-up approach).

I will focus on each of these elements in a greater detail to see whether, and to what extent, ownership of personal data in IoT is compatible with the top-down or bottom-up approach, and what limitations for explaining and justifying the introduction of ownership of personal data these approaches have. Supposedly, when discussing reasons for introducing ownership of personal data,[45] as opposed to reasons for introducing just a partial aspect of data ownership, one should be able to explain all four elements, because only if we can explain why it is desirable to create stably these four elements or to bestow stability upon all these four elements, we have a justifying cause for introducing legal ownership as a whole.

3.2.1. *Control of personal data*

Ownership *qua* full-blown control makes it possible for the owner to use the personal data fully, i.e. to access, store, share, sell, and amend them, or to process these data to turn them into all sorts of meaningful (and even non-personal) information. It also allows the owner(s) to destroy or abandon the data and implies responsibility for what may be caused to others when exercising this control, much in the same way a car owner is ultimately responsible for damage caused by his/her car.

In the top-down approach, the desirability of ownership-like individual control of personal data is most often explained in economic terms. The European Commission, for example, takes such overarching macroeconomic explanation as its starting point. It clearly states that 'if policy and legal framework [including data ownership framework] conditions for the

[42] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* EU:C:2011:771; J Wagner and N Witzleb, '"Personal Information" in the Australian Privacy Act and the Classification of IP Addresses' (2017) 4 EDPLR 528.

[43] Floridi (n 28) 354; Floridi (n 29).

[44] Waldron (n 21) 2; Mattei (n 18) 4. With regard to personal data, e.g., Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence' (n 30) 39.

[45] A good summary of individual reasons for and against introduction of data ownership can be found eg in Osborne Clarke LLP (n 6), reviewing national academic debates in Europe, or in Purtova, *Property Rights in Personal Data: A European Perspective* (n 30) 129–51 (alternatively Purtova, 'Property rights in personal data: Learning from the American discourse' (n 30), reviewing academic debates in the US.

data economy are put in place in time, its value will increase to EUR 643 billion by 2020, representing 3.17% of the overall EU GDP'.[46] The Commission also embraces data ownership as a legal tool facilitating access, free flow, and portability of data and a top-down instrument that might enhance competitiveness and innovation in data economy.[47] The top-down economic arguments also dominated the US debate on propertisation of personal data.[48] These top-down explanations fall short, however, of explaining why ownership-like control is best suited to achieve said economic and factual goals as opposed to other models of data control, which is a critique that has been raised repeatedly.[49]

The demand for ownership-like type of control can thus be explained more convincingly by the bottom-up approach. The typical bottom-up reasons featuring in the ownership debate are that *de facto* control is already in place thanks to existing technologies, such as the Personal Information Management systems,[50] as well as thanks to legal tools, such as the right to data portability[51] and the duty to obtain informed consent before personal data can be collected and used.[52] There are also more normative arguments supporting the bottom-up approach, such as that an individual has a natural right to informational self-determination regardless of the positive laws.[53] These pre-positive (i.e. bottom-up) reasons are then supposed to explain why it is desirable to bestow stability upon existing control of personal data by introducing their ownership and thereby 'unlock[ing] the full potential of IoT' for every such *de facto* owner.[54]

The bottom-up approach is, however, also facing some serious difficulties. One is that informational self-determination and personal data control (if seen as fundamental rights) conflict with inalienability of fundamental rights. According to this critique, personal data cannot be factually controlled in full.[55] Moreover, this fundamental rights' view discriminates against default allocation of ownership of personal data to anyone else than to the data subjects. Those accounts that look at factual control over personal data no matter what the normative grounding of such control face two closely related problems. For one, they cannot talk about *de facto* full control because data protection rules such as the GDPR already restrict the potential scope for control. Secondly, even if data protection rules were not in place, IoT architectures make it practically impossible to exercise full-blown factual control over personal data. In the IoT systems, the same *type* of personal data can have multiple *tokens* (copies) and no one does (for the time being) control all the tokens. It is thus hard to see personal data as a rivalrous and therefore exclusively controlled object. Moreover, the built-in cloud layer of IoT systems demands us to deal with problems of comprehensive control of data in the cloud.[56] This issue needs to be addressed at a technological level first, without any prejudice towards the optimal model of allocation of such ownership.[57]

3.2.2. *Protection of personal data*

The passive aspect of ownership rights embodies the interest in excluding others from controlling personal data[58] and the interest in having a legal remedy when someone infringes the data.[59] Since the passive and active aspects of ownership rights are two sides of the same coin, the arguments presented in previous section apply here too. A couple of additional remarks needs to be made, though, because the protective aspect of ownership closely relates to the issue of privacy and because, as we have seen in Section 2.2, privacy concerns perplex the debates on ownership of personal data.

Reasons supporting desirability of ownership of personal data at large, i.e. potentially *anyone's alienable* right to ownership of such data, are often mixed with privacy reasons supporting desirability of only *data subject's unalienable* right to ownership of his/her personal data. Although intertwined, these two groups of reason differ in at least one aspect that is crucial for ownership debates. Both rules regulating ownership of personal data and rules regulating protection of personal data necessarily relate to personal data. So far, they are intertwined. Yet ownership protection must relate to personal data *qua* an ultimate object of ownership rights,[60] and not to personal data *qua* an intermediary tool of protecting personal information and personality rights. So far, they differ. The arguments explaining desirability of ownership of personal data must, therefore, focus on the *data* aspect of personal data, as opposed to the *personal* dimension of personal data. This overlap of the economic, market-oriented approach to personal *data*, and the privacy-oriented approach to *personal* data can

[46] Commission, 'Building a European Data Economy' (n 6) 1.
[47] ibid 11.
[48] Purtova, *Property Rights in Personal Data: A European Perspective* (n 30) 133ff; Purtova, 'Property rights in personal data: Learning from the American discourse' (n 30) 507, 515ff.
[49] Drexl and others (n 3) 2–3; Osborne Clarke LLP (n 6) 62.
[50] European Data Protection Supervisor (n 15).
[51] P De Hert and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 CLSRev 193, 201.
[52] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Development on the Internet of Things' (WP 223, 16 September 2014) 6, 13.
[53] V Mayer-Schőnberger, 'Data Protection in Europe' in PE Agre and M Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997) 229–32; O Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 195; Osborne Clarke LLP (n 6) 60.
[54] McKinsey Global Institute (n 1) 11.
[55] Lynskey (n 53) 240–44; Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence' (n 30) 59; Osborne Clarke LLP (n 6) 58–59.
[56] Bartolini, Santos and Ullrich (n 5); N Ambika and M Sujaritha, 'A Data Ownership Privacy Provider Framework in Cloud Computing' (2017) 2 IJSRCSEIT 462.
[57] e.g., S Sicari and others, 'A security-and quality-aware system architecture for Internet of Things' (2016) 18 Inf Syst Front 665; S Sicari and others, 'Security, privacy and trust in Internet of Things: The road ahead' (2015) 76 Computer Networks 146; A Mashhadi, F Kawsar and UG Acer, 'Human Data Interaction in IoT: The ownership aspect' (2014) IEEE World Forum on Internet of Things (WF-IoT) 159; AM Al-Khouri, 'Data ownership: who owns "my data"' (2012) 2 International Journal of Management & Information Technology 1.
[58] e.g., Commission, 'On the free flow of data …' (n 6) 11, 33, 35.
[59] Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence' (n 30) 56–58.
[60] See van Erp (n 6).

be illustrated, for example, by the overlapping EU competition and data protection laws.[61]

If we look away from the wealth of privacy-oriented arguments featuring the debates about ownership of personal data,[62] we are not left with much more than utilitarian arguments according to which full-blown protection of personal data promises more efficient use of services, bigger consumption, and increasing macroeconomic figures.[63] These arguments stem from the top down and their limitations were mentioned earlier. Still, in the IoT context, the top-down approach seeks to offer additional explanation of why ownership-like protection is desirable. Some argue that ownership of data created by IoT is needed because the current legal framework for copyright, database rights, know-how, trade secrets, as well as for general data protection does not *comprehensively* govern these questions.[64] Such reasoning, however, only aims at a new model of protection and does explain why this issue should be dealt with comprehensively in the first place.[65] In my view, therefore, the present debates on ownership-like protection of personal data are framed from the top down implausibly.

The bottom-up approach, in contrast, has strong footing in factual evidence. The data subjects can, on one hand, effectively exclude others from collecting or processing personal data relating to them by, for example, not even providing the primary data or by not consenting to collection or processing of these data. On the other hand, it is presumed that personal data collectors and processor can already *de facto* exclude others from using and accessing the data, which was one of the reasons why the right to erasure of data and the right to data portability were vested in Articles 16 and 20 of the GDPR.[66] Hence, the explanatory power of the bottom-up approach to ownership of personal clearly outperforms the top-down alternative.

One practical limitation for both the top-down and bottom-up approach to ownership-like protection of personal data is that the existing IoT architectures do not (yet) provide technological solutions to the so-called 'transparency test' of ownership. Transparency is an essential feature of ownership thanks to which a given object (property) can be efficiently protected against everyone (the *erga omnes/in rem* feature of ownership) because everyone has 'an adequate possibility of finding out whether any property rights [transparently] exist for a given object'.[67] Nevertheless, considering how complicated it is to define personal data conceptually, let alone technologically, and considering the nature of data flow in IoT environments, it is currently implausible to expect that the law could offer stabile protection over personal data themselves. More research is thus needed to define how personal data transparently manifest themselves to potential wrongdoers in IoT, or how they can be made transparent to them so that the potential wrongdoing can be prevented and that some standard of reasonable care can be established in these contexts. Suffice to add that in order to exercise full-blown control over personal data (the active aspect of ownership) the data so controlled do not necessarily need to be transparent to anyone except for the owner, and so this problem only concerns the passive aspect of ownership.

3.2.3. *Valuation of personal data*

The issue of transparency feeds directly into valuation of personal data, because personal data must ultimately have some manifested utility and transparent value for their potential owners. It must therefore be possible to embody this value in personal data as into a tradable, controllable, and protection-worthy commodity.[68] At least in principle, thus, it must be possible to achieve transparent valuation of personal data if we want to justify desirability of their ownership.

From the top-down perspective, it is tempting to create stabile valuation of personal data because on the macroeconomic level the usage of personal data boosts economic growth and incentivizes innovation. The usual line of top-down arguments thus implies that personal data have some intrinsic utility or economic value. In the light of the economic success of Big Data companies, it is generally assumed that data, including personal data, are the new oil or gold of the data economy and must therefore embody tremendous and increasing value. In this light, valuating personal data by creating a right to ownership in relation to them promises to secure their universal and stabile worth.

The top-down implication that vesting value in personal data is desirable is inconclusive though. As for example the OECD report states, data themselves have no intrinsic value and 'their value depends on the context of their use' as well as on how personal information can be extracted from them.[69] The top-down approach is thus unable to explain why value (and its ownership-like protection) should be vested in the data rather than, for example, in the analytic algorithms or innovative businesses that make use of these data. In the IoT context, this means that the top-down approach can convincingly explain only desirability of ownership of larger functional units, such as the elements of IoT physical infrastructure, but cannot explain why it is also necessary to treat the data themselves as an elementary unit of value. The same line

[61] F Costa-Cabral and O Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 CML Rev 11. See also N Helberger, FJ Zuiderveen Borgesius and A Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 CML Rev 1427.

[62] See, e.g., Lynskey (n 53) 194ff, 231ff.

[63] See Commission, 'Building a European Data Economy' (n 6) 1, 3, 33; OECD, *Data Driven Innovation: Big Data for Growth and Well-Being* (OECD 2015) 195; P Bernt Hugenholtz, 'Data Property in the System of Intellectual Property Law' in Lohsse, Schulze and Staudenmayer (eds) (n 6) 79.

[64] e.g., Farkas (n 5) 11; De Franceschi and Lehmann (n 30); JAT Fairfield, *Owned: Property, Privacy, and the New Digital Serfdom* (CUP 2017) 236–38; PM Schwartz, 'Property, privacy, and personal data' (2004) 117 HarvLRev 2056.

[65] cf Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence' (n 30) 56–58.

[66] cf N Purtova, 'The illusion of personal data as no one's property' (2015) 7 Law, Innovation and Technology 83, 109.

[67] van Erp (n 6) 239. See also Thouvenin, Weber and Früh (n 6) 134.

[68] e.g., World Economic Forum (n 13); C Langhake and M Schmidt-Kessel, 'Consumer Data as Consideration' (2015) EuCML 218; Wendehorst (n 11) 330.

[69] OECD (n 63) 197.

of reasoning was taken by the European Commission when it suggested that those who own data collecting or processing tools could have sufficient claim on ownership of the data because they make substantial investments at a higher functional level and thus (indirectly) vest value in data.[70] Interestingly enough, the Commission did not see this as an argument against ownership of data as such.

From the bottom-up perspective, personal data are considered clearly valuable in themselves.[71] This can be demonstrated by the existence of data brokers who sell personal data analogically to how other brokers sell various raw commodities on the gamut from crude oil to gold. Therefore, in the bottom-up approach, the metaphor for personal data as tradable commodity stands. Property is embedded in the EU law and national legal systems as something valuable in itself and, in this respect, personal data are no different. Politics and scholars jointly acknowledge strategic, personal, political, economic, and many other types of worth embodied in personal data.[72] The fact is that, for the time being, value of personal data is considered indubitable and the introduction of ownership towards this asset is thus better explicable from the bottom-up. Nevertheless, even in the bottom-up approach it is often problematic to tell whether the valuable asset is a personal data set, each individual personal datum, or even personal information.

3.2.4. *Allocation of personal data*

The preceding three elements can jointly justify why the law should introduce ownership of personal data, i.e. why personal data should be qualified as property in legal sense. Let us assume that the reasons for propertisation of personal data are conclusive. It remains to be answered to whom these personal data should be allocated. As Purtova notes, 'as long as personal data bear high economic value – the real question is not "if there should be property rights in personal data", but "whose they should be" '.[73]

When discussing allocation of ownership rights relating to personal data, the most usual starting level of abstraction at which one defines potential owners is that it either should be the data subject, or not.[74] This dilemma stems normatively from the clash between the fundamental human right to respect of private life (substantiating the popular belief that personal data *should* be owned by the data subject in the first instance)[75] and the fundamental right to ownership (substantiating the view that allocation of ownership should be based on an egalitarian non-discriminatory test that applies to everyone, including the data subjects). The right to ownership of personal data should not, of course, neglect privacy demands. Yet it is possible, and even necessary, to put these fundamental personality rights in front of a bracket—keeping in mind that if the owner of personal data infringes these rights a remedy must always be in place—and to step into the brackets on a different level of abstraction where the allocation of ownership takes form of a universally applicable rule. In doing so, it is good to remind ourselves that ownership of personal data must be refined to ownership of extrinsically personal data. For the reasons just put in front of the bracket, it does not make sense to analyse ownership with regard to personal data that carry personal information about the data subject intrinsically. As was explained earlier, a mere retention of intrinsically personal data constitutes violation of the right to privacy as set out in Article 8 of the European Convention on Human Rights. If refined to only extrinsically personal data, the conviction that personal data belong or should belong to data subjects in some fundamental and perhaps also natural sense loses its explanatory and justificatory grounds and remains open to revisions.

At the correct level of abstraction, i.e. where the allocation of ownership conforms to a universal rule, we can, again, adopt both the top-down and bottom-up approach to how we explain this rule. The debates on ownership of personal data offer a plethora of candidates that are put forth as being best suited for the initial allocation of ownership of data (e.g. data producers, creators, consumers, compilers, enterprises, funders, decoders, etc.).[76] These debates, however, do not explicitly formulate any universal rule for such allocation and, although they correctly put personality rights in front of the bracket, they still do not attain the desired level of abstraction. The European Commission, for example, only vaguely expressed that 'the allocation […] of the right [to ownership …] would be guided by a thorough analysis of all elements relevant for allocating such a right'.[77] Clearly, thus, exploration of the two approaches in relation to allocation of personal data at the correct level is needed.

In the top-down perspective, one can imagine various distributive models of ownership allocation depending on what authoritatively posited public interest shall be satisfied by such allocation or what goal is the allocation meant to achieve. From the top-down, one can introduce state or communal ownership of personal data[78] as easily as private ownership. The top-down explanatory reasons might stem from economic policies, considerations of consumer welfare, innovation strategies, competition policies, or social security goals. In more general terms, any particular model of allocation would be thus reasoned by some policy reasons and goals. The current EU policies embrace a prosperous digital economy—which is a goal that could favour ownership of entities that can make best economic use of the data. A more refined definition of such entities exceeds this paper's ambit, but it can be expected that legislative bodies would be able to identify them by conducting a regulatory impact assessment.

[70] Commission, 'On the free flow of data …' (n 6) 35.
[71] Osborne Clarke LLP (n 6) 47–48.
[72] See, e.g., Commission, 'Building a European Data Economy' (n 6); Lohsse, Schulze and Staudenmayer (eds) (n 6); van Erp (n 6) 241; Rees (n 23) 75; Al-Khouri (n 57) 2; Farkas (n 5); Purtova, *Property Rights in Personal Data: A European Perspective* (n 30) 132–33.
[73] Purtova, 'The illusion of personal data as no one's property' (n 66) 109.
[74] Similarly, see J Kang and B Buchner, 'Privacy in Atlantis' (2004) 18 HarvJL& Tech 229, 238 fn 37.
[75] See literature in n 6; Rees (n 23); Mashhadi, Kawsar and Acer (n 57); Al-Khouri (n 57).
[76] OECD (n 63) 196; Osborne Clarke LLP (n 6) 75; Bernt Hugenholtz (n 63) 81.
[77] Commission, 'On the free flow of data …' (n 6) 34.
[78] e.g., M van Alstyne, E Brynjolfsson and S Madnick, 'Why not one big database? Principles for data ownership' (1995) 15 Decision Support Systems 267.

The bottom-up approach to allocation of ownership of personal data can be expanded in more detail since the philosophy of property law already came up with three bottom-up theories advocating three distinct types of universal rule on *who* should be the owner of some property. My analysis, therefore, will make use of these three theories: (a) the first occupancy/first labour (or simply Nozickian) theories; (b) the pure force/last occupancy theories; and (c) the Humean theories.[79]

3.2.4.1. *Nozickian theories* The Nozickian theories commit to two principles: (i) a person who first does an activity χ in relation to a resource D (e.g. data) is the owner of D and (ii) the first owner of D can voluntarily transfer this ownership to another person, who will then become the new owner of D. According to (i), the *first* ownership of D is explicable as a unilateral acquisition and is justifiable by the owner's doing of χ. According to (ii), any non-first ownership is explicable as being transferred from one owner to another, and is justified recursively by each previous transfer and by the first owner's activity χ in relation to D. For some, such as Locke, the χ activity is labour; for others, such as Pufendorf, the χ activity is occupancy.[80]

When it comes to ownership of personal data in IoT, we may conceptualize the activity χ as collection of personal data. Under this interpretation, when data are collected, they become a potential source of further activities such as harvesting the value of the data by extracting the personal information from them. Therefore, just like with first labour or occupancy, those who *first* collect the data are best entitled to keep their possession, because without them the data would not be existent in the IoT environments. On this account, all personal data seem to be explicable and justifiable as belonging to the data collectors because they first do χ in relation to them. This interpretation also aligns with the EU law distinction between data created by some entity (typically machine-generated data) and collection of independently existing data (typically sensory data).[81]

In a more refined interpretation, though, we can say that personal data originate because of the harvesting activity. The difference between collection and harvesting of data being a difference between massively collecting data by sensors of IoT devices and cherry-picking personal data from this mass of data by harvesting their informational value. Under this interpretation, the harvesting activity could include generating derivative personal data extracted from the primary data sets or generating personal metadata. On this account, we can explain allocation of personal data to anyone who harvests them. It can be some qualified data collectors (harvesters), but it can be also data subjects who generate the valuable 'cherries' made of personal data (e.g. by filling out questionnaires or forms and thereby feeding the IoT environments with their personal data directly; or simply by uploading some packets containing personal data). Here, the data subjects must actively generate the relevant data for the IoT environments and such activity χ is thus a sufficient reason for them to believe that the data can be theirs. In other scenarios, the first harvesters will be different and a priori indeterminate, which is an explanatory advantage of this theory.

The second Nozickian principle—explaining and justifying ownership by transfer—faces some fundamental obstacles in IoT. The key challenge is that data are being transmitted almost instantly, and so they change hands at all times. According to Zech, this is not an issue because 'using data by analysing them can be done relatively quickly'[82] and so even a short-term ownership-like protection is appropriate for this purpose. Another obstacle is that personal data can be copied, multiplied, and mixed with other data and modified (for the purposes of standardization and interoperability). These specifics make it technically very complicated to trace the data transactions and to locate the personal data themselves. However, the Nozickian theories of ownership could work in scenarios that would allow such tracking of data (e.g. by implementing blockchain technologies). Where this tracking would not be possible, e.g. because of high costs of the technological solution, a legal fiction of first ownership of the harvester could be introduced, yet this would depart fundamentally from the Nozickian model. In fact, it would be a top-down solution.

3.2.4.2. *Pure force/last occupancy theories* The pure force or last occupancy theories explain allocation of ownership simply by looking at the *last* owner. In plain terms, ownership exists for the benefit of those who get last to gain control of the valuable resource D, usually by means of pure force or just by occupying the resource D. As Waldron observes,

> the powerful and the cunning [… who] manage to hold on to the things they have [successfully] grabbed [by using force …] use their power, politically, to persuade the whole society to throw its force behind their depredations.[83]

When *de jure* ownership enters the official legal system, it consolidates the existing rights of the last *de facto* owner.

One obstacle for these theories, similarly to the previous group of theories, comes from the nature of IoT systems where the same *type* of personal data can have multiple *tokens*. This makes it practically impossible to say who is the *last* holder of the data (as a type) unless we want to permit data co-ownership. Moreover, if we take into consideration the essential component of all IoT—cloud computing (i.e. a layer where data are processed and often mixed together)—then this bottom-up theory retains practically no explanatory power regarding ownership of personal data. Unless the ownership issues in the cloud layer will be regulated separately by a set of special rules, it seems impossible to apply this theory to anyone's last factual ownership because there is no clear last factual owner of the data. At best, data would have a new

[79] Waldron (n 21) 6.
[80] In short, see ibid 2–4.
[81] Case C–203/02 *British Horseracing* EU:C:2004:695. See also M Leistner, 'Big Data and EU Database Diretive 96/9/EC' in Lohsse, Schulze and Staudenmayer (eds) (n 6) 28.
[82] H Zech, 'Data as a Tradeable Commodity' in A De Franceschi (ed), *European Contract Law and the Digital Single Market* (Intersentia 2016) 76. Surprisingly, both Bernt Hugenholtz (n 63) 82 and Commission, 'On the free flow of data …' (n 6) 23 refer to this source as to 'Information as a Tradable Commodity', which further demonstrates the confusion between the concepts of data and information (see Section 2.2).
[83] Waldron (n 21) 5.

factual owner at each stage of its IoT-life-cycle, thus demanding of us to alter our understanding of stability of *de jure* ownership into some form of fractional stability where each stage features stability for only a minimal time-span.

Another problem is that these theories are considered 'morally bankrupt',[84] for they only aspire to explain the origin of ownership but not to justify it. This makes it harder, albeit not impossible, to appeal to these theories. With regard to intangible personal data (and data in general) which are non-rivalrous by definition, we can imagine that, in principle, every single person could eventually come into the last possession of personal data because every token of the same type of personal data may end up in the hands of a different owner and may be copied infinitely. If we accept the idea that the same type of personal data can be occupied by multiple token-owners in parallel, then this theory does not need to be morally bankrupt. In fact, it is better able to explain why *someone* shall own personal data (by factually taking them and possessing them) and may be justified by his/her ability to do so. Accordingly, this model can offer more realistic explanation of data ownership than the Nozickian theory because it refers to the last factual holdings of data and not to a historical myth of the first ownership—a myth that would often be problematic to prove by evidence.

A general problem of this theoretical explanation is that unless we restrict the object of ownership to personal data as tokens, this theory undermines the excludability feature of ownership because exclusion cannot be achieved at the level of data as a type. At the same time, if we restrict the object of ownership to data as tokens, there remains a danger that big players will restrict the number of these tokens and monopolize the market in personal data. To give an example, such last *de facto* owner of data tokens could be Telefónica which controls the AURA platform. Telefónica presumably gives control over personal data to the data subjects but *de facto* exercises the control over the individual data tokens itself. If designated as a rightful legal owner of personal data, Telefónica can then easily exclude other service providers from using the data tokens simply by taking advantage of its AURA platform.

3.2.4.3. Humean theories According to Hume, property exists to allow us to enjoy peacefully our possessions similarly (as far as possible) to how we enjoy our mental and bodily advantages. Our need for ownership is therefore justified by a natural tendency to have stabile possession of things 'which we call external'[85] and of which we make use in our lives.

Such a broad theory, on the one hand, explains our need for creating data ownership (or at least to possess data factually). Yet, on the other hand, it is too demanding on the types of data that might be so controlled. Namely, by invoking the analogy between peaceful possession of ourselves (mind and body) and the desire to exercise the same degree of control regarding external things, it restricts itself to explanation of ownership of external things. Now the trouble with personal data is whether they can be, under this theory, conceptualized as *external* things. As I have already argued in section on personal data (Section 2.2), ownership can be considered only in relation to data that do not intrinsically contain personal information. The Humean theories, then, additionally restrict the scope of personal data ownership to things external relative to our minds and bodies. One may argue that such external personal data could be interpreted as extrinsically personal data such as your GPS location, your IP address, or data in your task manager. However, for this theory to work, the externality aspect of personal data would need to be explored in more detail.

Under Humean theories, the origin of ownership is justified by common sense and not by an arbitrary ownership-like status acquired by use of pure force—which is a difference in comparison with the previous theories. Ownership originates from the instability of possessions of external goods and is underpinned by the interests of *all* owners and members of the society, not only those who are powerful and can occupy the data. According to Hume, peaceful possessions (ownership rights) are secured by

> a convention enter'd into by all the members of the society [… But the t]his convention is not of the nature of a promise [like with classical contracts. … Instead, i]t is only a general sense of common interest; which sense all the members of the society express to one another, and which induces them to regulate their conduct by certain rules.[86]

Thus, data ownership would first need to be commonly agreed to by those who have interests in control, protection and valuation of personal data, and only then could it be translated into the official system of laws. Thanks to this justification, this theory can additionally explain, in comparison with the previous theories, also the allocation of ownership of personal data as a type. I suspect, however, that the time when such common sense would be apparent to all of us is yet to come.

3.3. *Limitations of the two approaches*

The two approaches to ownership of personal data have each some explanatory advantages and disadvantages in respect of the four elements of ownership (control, protection, valuation, allocation). Table 1 summarizes their ability to explain these individual justifying elements.

If analysed at a more general level, both approaches to ownership of personal data in IoT have additional limitations. The major limitation for the top-down approach stems from the doctrinal nature of any such approached model of ownership of personal data. According to Article 345 of the Treaty on the Functioning of the European Union (TFEU), the EU does not formally have the authority to posit data ownership as a new type of right. Property ownership is explicitly excluded from the powers conferred upon the EU,[87] and so it is impossible to imagine that this type of new doctrinal *legal* right could originate by a top-down authoritative act of the EU. The current EU laws simply do not leave room for top-down creation of a legal

[84] ibid 5.

[85] D Hume, *Treatise of Human Nature* (1739–40) Bk III, Part ii, section 2.

[86] ibid.

[87] 'The Treaties shall in no way prejudice the rules in Member States governing the system of property ownership.' This was the case also in the Treaty of Rome 1957, Art 295.

Table 1 – Limitations of the top-down and bottom-up approaches.

			Explanatory approaches	
			Top-down	*Bottom-up*
Justifying elements	*Control*	+	Macroeconomic growth & innovation	Factual control already in place in some contexts
		–	Unclear why ownership is the best legal tool to achieve these goals	Cannot explain full control (limiting natural rights and data as tokens)
	Protection	+	See above + lack of comprehensive protection	Factual protection already in place in some contexts
		–	See above + unclear why comprehensive protection + transparency issues	Protected rights in data are not transparent to third parties
	Valuation	+	Macroeconomic growth & innovation	Reflects strategic, personal, political, and economic value
		–	Insufficient for explaining data as the smallest value unit	Unclear what is valuable (personal data/information/datum)
	Allocation	+	Aligns with policies and public goals	Strong theoretical background (Nozickian, pure force/last occupancy, Humean)
		–	Indeterminate allocation without impact assessment	No single theory is completely sufficient in the IoT context

(+ explanatory advantages; – explanatory disadvantages)

right to ownership of personal data. It would only be possible if data ownership was categorized as intellectual property (IP), because Article 118 of the TFEU empowers legislative bodies of the EU to 'establish measures for the creation of European intellectual property rights to provide uniform protection of intellectual property rights throughout the Union'.[88] There is, however, no convincing reason to assume that data ownership belongs to IP law rather than to any other area of law, albeit data are currently protected as part of database rights (IP-law protection) and they convey IP-law protected information (copyright, trademarks, know-how, trade secrets). This unreasoned assumption, implicitly present in many academic writings,[89] shall be rebutted until more convincing arguments will be put forth. In fact, the European Commission expressly did not want data ownership to be any 'super-IP right' either.[90]

The second limitation for the top-down approach follows from the rhetoric that ownership discourse reinforces at both the EU and Member States' level and that conceptualizes ownership of property and the right to personal data protection as fundamental rights, thereby as something pre-positive.[91] The rhetoric of fundamental rights expresses the belief that ownership cannot stem from formal authorities but must stem from the human nature. This is a conviction that has transformed the European political and legal landscape some 200 years ago, and it was already present, for example, in Locke's theory of ownership. In the *Second Treatise of Government*, Locke wrote: 'it is very clear, that God, as king David says, Psal. CXV. 16. has given the earth to the children of men; given it to mankind in common',[92] and '[t]he reason why men enter into society, is the preservation of their property'.[93] If we accept this narrative, then '[i]n the state of nature, all particular things [including data] are unowned'.[94] In this sense, data—as potential objects of our possession—have always existed in the world for us to be possessed and the new data-mining techniques and economic models do not undermine the underlying explanation so neatly invoked by John Locke. Thus, putting aside questions such as the nature of data, the nature of owners and the question whether this narrative is only an illusion,[95] 'the correct starting point is the Lockean position that [any] property rights come from the bottom up'.[96] Under this rhetoric, one would find any top-down regulation of ownership as an axiomatically unjustified restriction on our natural rights to own personal data, which leads to further justificatory and ethical problems.[97]

The third limitation, partly factual and partly conceptual, comes from the motivations behind the current discussions and proposals on data ownership. If we look at them, we soon realize that the rationale for introducing ownership is most often rooted in non-positive and non-authoritative notions such as human rights, privacy, free flow of data, or data portability. Data ownership, according to this factual evidence, is then meant as a regulatory response to the problems and concepts that stem from the bottom up and not vice versa. Given the ubiquity and cross-jurisdictional nature of IoT and data

[88] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326/47, Art 118.

[89] e.g., Farkas (n 5); Gärtner and Brimsted (n 6); Bernt Hugenholtz (n 63) 77–81.

[90] Commission, 'On the free flow of data …' (n 6) 34.

[91] See the Charter of Fundamental Rights of the European Union [2012] OJ C326/391, Arts 8(1) and 17(1); TEU, Art 39; TFEU, Art 16; Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms Paris (1952), Art 1.

[92] J Locke, *Second Treatise of Government* (first published 1690, CB Macpherson ed, Hackett 1980) § 25.

[93] ibid § 222.

[94] RA Epstein, *Design for Liberty: Private Property, Public Administration, and the Rule of Law* (Harvard UP 2011) 99.

[95] J Litman, 'Information Privacy/Information Property' (2000) 52 Stan L Rev 1283, 1292.

[96] Epstein (n 94) 99.

[97] cf Van den Hoven (n 2) 11–12.

flows, it would in fact make little sense to design an a priori top-down model of data ownership regardless of the factual evidence. Instead, such an approach would most likely prompt new problems. For example, it could lead to some sort of centrally planned data economy—which would be falsely justified (as other top-down theories) by the tragedy of the commons and by the necessity of regulation over scarce resources.[98] The digital commons, however, invoke a specific type of tragedy[99] and so we have to tune our reasoning accordingly. At first glance, data, including personal data, are anything but scarce and so their centralized or authoritative distribution would be unjustified unless the technology, for example, makes them scarce. Conceptually though, it is once again important to distinguish between scarcity relating to personal data as a *type* and personal data as a *token*. A top-down regulation can thus make sense only at the *type* level. This limitation clearly demands further unpacking which exceeds the scope of this article.

Overall, ownership of personal data cannot be authoritatively created at national or supranational level, because the purpose of creating data ownership, the nature of ownership, and the nature of personal data as an object of ownership are all unfit the top-down explanations and justifications. And so, if the top-down approach cannot explain all four elements of ownership, it cannot succeed in relation to ownership of personal data at large too. If this argument is sound, then all the existing top-down explanations must in fact be explaining something different from ownership of personal data, albeit they do so under the veil of ownership terminology. This is something we should openly acknowledge.

As to the bottom-up approach, the preceding analysis suggests that the core reasons for introducing ownership of personal data can only be approached this way. Yet as we have seen, it also has some explanatory limitations regarding individual elements of ownership of personal data in IoT. At a more general level, the major limitations for the bottom-up approach are ethical. The emerging unregulated *de facto* ownership of personal data can progress via ethically problematic (if not unethical) routes, be it via unfair commercial practices, restriction on free access to some data, informational propaganda, discrimination, or identity fraud. These reasons, nevertheless, do not speak strictly against the bottom-up approach to introduction of ownership and so, unless debates on ownership of personal data are to be repealed due to these ethical risks, the preferred perspective is the bottom-up one.

4. A revised (bottom-up) approach to ownership of personal data in IoT

Although the bottom-up approach came up as the preferred variant, it is far from being perfect. On the contrary, it faces serious explanatory difficulties, mainly due to the specificity of personal data and IoT. It is thus useful to outline some basic features that any upcoming bottom-up approach to ownership of personal data should bear in order to meet these challenges.

To explain all four elements of ownership of (extrinsically) personal data from the bottom up, we firstly need to be able to address the problem of full control regarding data tokens and to explore whether and how it could be feasible. That will be a legal, philosophical, as well as technological challenge.

Secondly, we need to address the problem of transparency of personal data as an object of ownership protection. This challenge will be primarily technological. It seems that until the necessary technological advancements will be at hand, ownership-like protection will remain inexplicable from the bottom-up perspective. In the context of everyday IoT (e.g. in smart cities) neither a factual owner nor a legal owner would be able to spot on whether her property was damaged, stolen, amended, or unjustly used. In turn, a putative wrongdoer would not know whether she interfered with someone's legal property. This problem can be addressed by bottom-up technological solutions such as the AURA platform or Solid.[100] By contrast, factual enforcement of ownership rights to data cannot be dealt with on the paper (a top-down model). Instead, it needs to be embedded in the hardware and software implementations of IoT.[101] The laws can set up a system of fictions and sanctions to facilitate such enforcement and incentivize the ownership system of personal data, yet such regulatory intervention would not explain, nor justify ownership at large.

Thirdly, although personal data are already considered valuable, there remains a similar technological challenge regarding how the valuation element of ownership can be vested transparently in personal data. Furthermore, at least a conceptual line between valuation of personal data, personal information, and a personal datum shall be considered more carefully.

Solutions to all these three issues must precede any bottom-up propertisation of personal data. Given the strong top-down as well as bottom-up economic incentives, we can expect though that they will be resolved (at least theoretically) in not that distant future.

A slightly separated issue is that of allocation. To explain to whom ownership of personal data should be allocated, it will be first necessary to abstract from personality rights and consider the question of allocation at the correct and unbiased level of abstraction. The criterion/criteria for allocation therefore cannot start with the assumption that the data subject has or should have any stronger claim on ownership of the data than anyone else. We saw, however, that bottom-up theories of ownership still do not comprehensively answer the allocation problem in the IoT context. It thus seems a productive strategy to keep reinterpreting these theories in the light of new technological, legal, and conceptual developments and to remain open to revisions of these interpretations. For now, we shall be ready to revise all three variants: (a) the Nozickian theories (where the main challenge will be conceptual with regard to interpretation of the first activity χ); (b) the pure force/last occupancy theories (where the main

[98] e.g., Mattei (n 18) 1.

[99] GM Greco and L Floridi, 'The Tragedy of the Digital Commons' (2004) 6 Ethics Inf Technol 73.

[100] Solid <https://solid.mit.edu/> [https://perma.cc/G4PW-8A43].

[101] e.g., S Tyagi, A Darwish and MY Khan, 'Managing computing infrastructure for IoT data' (2014) 4 Advances in Internet of Things 29.

challenge will be conceptual and legal with regard to definition of personal data types/tokens); (c) the Humean theories (where the main challenges will be conceptual with regard to extrinsic/external personal data, and empirical with regard to presumptive claims about common sense).

5. Conclusion

We have seen that ownership of personal data cannot be comprehensively explained and justified by any of the two approaches to ownership (bottom-up and top-down). While the top-down approach proved to be fully unfit for explaining and justifying ownership of personal data in IoT at a general level, and partly unfit for explaining the issues related to control, protection, valuation, and allocation of personal data in IoT, the bottom-up approach was partly successful on both fronts.

To meet further challenges of the bottom-up approach, I argued for a revised version of a bottom-up explanation and justification of ownership of personal data. If this novel approach is to succeed, though, it must be better able to encompass conceptually personal data as potential objects of ownership rights and IoT as the key future environment for data transactions. Conceptually, this means to disambiguate information from data and to consider ownership exclusively in respect of data. This was my first original claim.

My second novel claim was that we must also disambiguate intrinsically personal data from extrinsically personal data. I argued that only the second category can be discussed as a potential object of ownership rights, and that these two categories shall not be replaced with the traditional duality between personal and non-personal data. In contrast with the existing literature, I argued that personal and non-personal data are not two conceptually incompatible notions.

The last original claim was that the popular question of 'Who owns the data?', i.e. the question of allocation of ownership rights to personal data, must abstract from privacy considerations. I argued that ownership allocation must employ some indiscriminate test that does not treat data subjects as a privileged category of potential owners. At the same time, I showed how this approach could be easily combined with protection of personality rights.

The outlined and revised approach to ownership of personal data in IoT can serve as a blueprint for future work in this area, should initiatives supporting ownership of data (including personal data) remain active, because it highlights key challenges concerning the elements of ownership of personal data in IoT. Yet it also shows that, since ownership of personal data still cannot be satisfactorily explained and justified, said initiatives should remain investigatory, analytic, and descriptive. So far, their stepping into the normative realm of '*should be introduced*' will be like stepping out of the frying pan into the fire.

Conflict of interest

The author declares no potential conflicts of interests.

Acknowledgement

This article is a deliverable of the 'PETRAS – Cybersecurity of the Internet of Things' project. The research on this project was funded by the Engineering and Physical Sciences Research Council (EPSRC), grant agreement no EP/N023013/1. The EPSRC played no role in study design; in the collection, analysis, and interpretation of data; in the writing of the article; and in the decision to submit the article for publication.

Thanks is due to Mariarosaria Taddeo for her comments and suggestions. All mistakes are mine.