Intelligent Environments 2018
I. Chatzigiannakis et al. (Eds.)

© 2018 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/978-1-61499-874-7-285

Governing Data Trade in Intelligent Environments: A Taxonomy of Possible Regulatory Regimes Between Property and Access Rights

Jacopo CIANI[a1]
[a]*University of Turin, Department of Law, Italy*

Abstract. Companies have been analyzing data from their own customer interactions on a smaller scale for many years. But only recently, they understood the potential treasure trove of non-traditional and less structured data (such as machine-generated data and social media data) that can be mined both for internal marketing purposes and for licensing to third parties.
From the business perspective, the protection of this data is needed to secure the significant economic investment that the "new data economy" can require. Otherwise, data holders may lack the incentives to share the data they own and control, because of the risk that non authorized users may "free ride" on their investment.
Granting property rights is often suggested as a solution to overcome the incentive problem. In the case of data, while relying on contract freedom may seem the favourite solution, between those extremes a spectrum of possible "halfway" approaches has been proposed. They range from "quasi-property" or "semi-commons", with a liability-like regime, to access rights, requiring to license extractions and reuse of data on FRAND terms.

Keyword. ambient intelligence, internet of things, digital single market, data-driven economy, data ownership, quasi-property, semi-commons, intellectual property rights, access

1. Setting the Stage of Ambient Intelligence

For the last two decades, scholars, journalist, and IT consultants, have been presaging what has been labelled the "ambient intelligence", a vision of a foreseeable future technological ecosystem where the human will be surrounded by a seamless environment of computing, advanced networking technology, and specific interfaces, enveloping the physical environment and distributing the technology focus and its computing power from computers to a multiplicity of everyday objects [1] [2].

The term was first used in 1998 in a series of workshops commissioned by consumer electronics company Philips [3] but was given its most significant boost as a key part of the European Commission's Sixth Framework Programme for Research and Technological Development in the area of Information Society Technologies [4].

[1] Scholarship holder, Ph.D. University of Milan, Associate at Tavella-Studio di Avvocati, Milan.

Not surprisingly in an area of innovation, the terminology used by researchers, industry participants and governments is not fixed. The expressions "Internet of things" [5], "Everyware" [6], "Ubiquitous" [7] or "Pervasive computing" [8] sometimes are used interchangeably, other times in different but overlapping contexts and with wider or narrower scopes of meaning [9].

Amidst the wide array of challenges posed by this vision of forthcoming reality [10], until now, the central question of research has been the impact of ambient intelligence (AmI) and of profiling techniques on individual autonomy and refined discrimination. Unauthorized and abusive access to the data collected, loss of control [11], dependency, social exclusion, unwanted and unwarranted surveillance, and more in general privacy [12], trust [13] and security concerns [14] [15] have been identified as possible disbenefits of these technologies [16] [17].

Others paid attention to the challenges that such technologies pose to the classical understanding, construction and concept of identity [18] [19], affected so intimately that many scholars refer to the multiplication of identities [20] and the digitisation or informationalisation of the human person [21], [22].

A special emphasis has been overall put by international [23] [24] and European policy [25-29] to the questions about ownership, access and trade in digital data that flow through the AmI, and potential data market failures that may require regulatory intervention.

Data and information are, by nature, non-rival. Many people can use the same data at the same time without any loss of information content for any of these parties. Even if I have it, it doesn't exclude you from having it too. The dramatic reduction in the cost of copying of digital content significantly reduces the natural excludability barriers conferred on information by its material carrier and raised questions about data free-riding [30].

Ensuring excludability requires technical and/or legal intervention to define and attribute exclusive property rights.

On the merits, an active legal debate has emerged, commenced in Germany, but soon become global.

The present contribution aims to add its voice to the debate, being structured in the following parts.

Whereas Sections 1-3 succinctly describe the Ambient Intelligence scenario, summarizing its main characteristics and features and introduce the data-ownership issue, Section 4 critically examines the traditional research focus on personal data and suggest that any analysis on the concept of ownership on data in the context of the Internet of Things (IoT) should be applied to all sorts of data (including non-personal).

In Sections 5-6 the article reviews existing legal frameworks dealing with data and describes the *status quo* where no ownership in data is formally assigned as a *de facto* property regime assigned to information industries with strong bargaining power.

An assessment on the legal instruments and landscapes which may affect commercial operator's access to and ownership rights over data is carried out in Sections 7-9, including a detailed discussion of forms of protection for commercially valuable data alternative to full-property.

Section 10 draws the conclusion that relying on contracts seem by far the favourite solution in the political, economic and academic fields, even if the Commission's investigations failed to reached a definitive position and called for more research to bring economics up to speed with this question.

2. Data as Engine of Revolution

Electronic systems, sensors and other objects distributed throughout the physical world via the constant monitoring of our actions and behaviour will, themselves, generate and produce massive amounts of personal data and information concerning our identity and behaviour.

This new stage has been possible by the passage from a model of people accessing internetworked computing services almost exclusively via a limited number of personal desktop computer to a "many people to many machines" model [31].

In this world where a wide array of miniaturised computing devices (processors, tags, tiny sensors) will be integrated into a multiplicity of everyday objects, software agents will work with an incomparable greater amount of information, captured not only through the websites we visit but also through the actions we make and the decisions we take in the physical world, including the conversations we have, the places we visit, the people we meet, the things we see, smell, eat and (even perhaps) think, among many other human activities.

The idea of such proactive instead of interactive computing [32] is that we need not provide deliberate input, but are 'read' by the environment that monitors our behaviour.

Control over such big amount of information is now increasingly possible thanks to the development known as "big data", which refers to gigantic digital datasets extensively analysed using computer algorithms [25] [33-34].

These technologies however only generate an enormous amount of data, which may not reveal any knowledge until profiling technologies are applied.

Profiling can be described as the process of knowledge discovery in databases, of which data mining (using mathematical techniques to detect relevant patterns) is a part [35], carried out by software programs trained to recover unexpected correlations in masses of data.

Profiling technologies are the crucial link between an overdose of trivial data about our movements and interactions with other people or things and applicable knowledge about our habits, preferences and the state of the environment.

Consequently, they generate new knowledge, or better discover knowledge that we did not know to be hidden in the data [36] [37].

Therefore, profiling creates an added value in a mass of data, of which we don't yet know what is noise and what is information [38]. The resulting new knowledge consists of group profiles which should indicate that all people with a specific mix of attributes entail a specific characteristic [39].

Data vendors sell access to their databases and data analytics to downstream firms which in turn use the data to improve their product positioning. Bergemann and Bonatti [40] distinguish three main types of data vendors depending on the source of the data: (1) financial data providers (Bloomberg or Thomson Reuters), including credit rating agencies (Equifax, Transunion, Moody's or Standard & Poor's); (2) Data brokers, e.g. LexisNexis and Acxiom, that compile huge databases on individual consumers from publicly accessible sources, e.g. social media, blogs and from their online purchases, browsing history [41]; (3) Online aggregators, e.g. Spokeo and Intelius, that mine publicly accessible data to create consumer profiles.

Other business models enable data owners to collect and commercialize the value of their data without selling (and revealing) them. It is the case of multi-sided markets

or platforms, as Amazon or e-Bay, which aggregate and analyze these data and use them to facilitate matching sellers and buyers.

3. Property Interests in Data

In any case, what is crucial in order to realize this economic value [24] is to ensure a possibility to make the data available to third parties on the basis of transfer or licence agreements.

A data owner can sign a contract with a data user that forbids any distribution to or re-use by third parties. However, that contract is not enforceable towards third parties who are not signatories to the contract. It is possible to obligate the licensee to ensure that any obligations under the data licence are also passed on to anybody who receives a sublicence. Furthermore, the licensor may be awarded direct contractual claims against such third parties. Otherwise, once the data are out in the open, the data owner has no legal means to enforce its rights.

In response to these challenges, a number of ownership-like types of technological solutions are emerging. One such example is the AURA platform—a Personal Information Management system (PIM) [42] —which was recently introduced by Telefónica in Spain and which allows end-users to control relevant data that their mobile operator holds about them (eg. the user's geolocation) and to decide with whom these data will be shared.

To that end, the Commission's 2017 Communication on Building a European Data Economy [26] considered the possibility of a legislation on a data producer's right as a possible way to incentive sharing data initiatives, enhance new business models for the exploitation of the data and unlock their economic value.

Understand who owns data, what possibilities exist for protecting against use by third parties and whether an hypothetical owner's right could coexist with the rights of data subjects in personal data under data protection law is considered «*a pivotal factor affecting a growing number of potential data users and an increasing range of data-related activities*», which plays «*a fundamental role in sustaining and developing the emergence of a European data-driven economy*» and is on the political agenda as part of the Digital Single Market Strategy for Europe [43].

On the contrary, an uncertain legal framework for data ownership, access, and trade inhibits the realisation of the full economic benefits of non-rival data.

It may potentially cause companies to hold back on data sharing initiatives and overcomplicates negotiations and restrict or slow down the extent of exploitation and innovation within data-driven industry sectors.

4. Setting the Scope of Data Ownership's Research

The legal debate on data ownership has been until now focused on the merits of granting full ownership rights to natural persons over their personal data. Several scholars have proposed allocating default entitlement of property rights on personal data to data subjects [44] [45] designed as a form of guarantee for data subjects' (human) rights, rather than as a regime of commercial exploitation of human identities

[46], due in part to the general refusal of a commodification of personal identities [47] [48].

Even after the legal developments in personal data protection, recently culminating in the GDPR, the situation is not apparently [45] [49] changed. The GDPR gives some specific rights to data subjects[2], but refrains from defining a residual ownership right in personal data. In any event, after the GDPR, it is more difficult to think of any data ownership, without also thinking about ownership of personal data [50].

This paper advocates that distinguishing between personal and non-personal data for the purpose of evaluating if any data ownership right would be appropriate is practically useless.

The recently issued proposal for a Regulation on a framework for the free-flow of non-personal data in the European Union (hereinafter the "Proposal") aims to put in place a comprehensive EU framework enabling free movement of data in the single market, "together with" the Union data protection legal framework, in particular Regulation 2016/679 (GDPR)[3]. That legal framework already ensures the free movement of personal data within the Union, so that the Proposal aims to complete such framework addressing the broader market for non-personal data storage and processing services and activities.

As a consequence, approaching the data ownership issue from the sole perspective of the legal regime of circulation of personal data is unnecessarily restrictive.

Of course, this does not amount to denying the differences between personal and non-personal data nor the impact of such differences on the circulation of data. But governing the mobility of data in the single market, placing - if needed - property rights on data (in general), does not affect in any event the obligations under data protection law under Regulation 2016/679 (GDPR). Hypothetically, personal data may be owned by data producers, controllers or processors, in the same way as non-personal data, but within the applicable limits imposed by the GDPR.

Therefore, it may be time to stop thinking in terms of ownership right in personal data and to focus research's attention on the legal regime that should better regulate collection, store, and transfer of all sorts of data (including non-personal) [51].

This focus of research follows the consideration that AmI is not only about personal data.

AmI systems don't need to identify a specific person in order to operate. For example, Fitbit's privacy policy stated that the technology produces "de-identified data that does not identify you", which may be used to "inform the health community about trends; for marketing and promotional use; or for sale to interested audiences"[4].

At the same time, the owner of the profiling system may have a strong incentive to make sure that the perception of movements, temperature, position, pressure remains anonymous as, in this case, relevant legal prescriptions, like the right of the subject to obtain information about the logic of any automatic processing of data concerning him, does not apply.

Moreover, identifying people with their precise names or addresses is becoming useless, since, in order to create a profile and to provide customized services, it may be

[2] including the right not to be subject to data processing without a legal basis, access, limited re-purposing, the right to be forgotten and the right to data portability.

[3] Proposal for a Regulation of the European Parliament and the Council on a framework for the free flow of non-personal data in the European Union, COM(2017) 495 final, pg. 3.

[4] Fitbit Privacy Policy of August 10, 2014, at www.fitbit.com.

sufficient to know, in some cases, only the categories to which a person is likely to belong [52].

As Pagallo [53] observes, Apple pioneered the incorporation of differential privacy techniques [54] in its data collection efforts for iOS and macOS, e.g. the reuse of health data through their apps for statistical purposes. The statistical purpose implies that the result of processing is not personal data[5].

Also Facebook uses differential privacy-supporting technologies to report audience reach data of its targeted advertising system [55][6].

As the aforementioned examples show, reasoning of data ownership in intelligent environments requires considering data as a whole, without focusing only on personal one.

5. The Current Normative Framework in relation to Data Ownership

At the current stage, ownership rights in data are only very partially defined. Most European countries do not have specific laws in relation to the ownership of data [56], besides, where applicable, copyright, database and trade secrets rights.

Such legislations, in any case, do not recognise a property right in data as such, rather, at most, provide for certain defensive rights which protect data against unauthorised access.

Neither it is possible to imagine that this type of right could originate by an authoritative act of the EU. According to Article 345 of the Treaty on the Functioning of the European Union (TFEU), "*the Treaties shall in no way prejudice the rules in Member States governing the system of property ownership*". Therefore, property ownership is explicitly excluded from the powers conferred upon the EU. It would only be possible if data ownership was categorised as intellectual property 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*". The European Commission however expressly excluded that data ownership may be configured as a "*super- IP right*" [27].

6. The Current State: a *de facto* Property Regime of Data

In the absence of legally specified ownership or residual rights, exclusive data ownership thereby becomes a *de facto* right allocated by the bargaining power distribution between parties [57]: who has the data can effectively prevent others from

[5] Recital 162 GDPR defines statistical purposes as "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results". The meaning of statistical purposes can be interpreted broadly and does not only cover uses for public interest but may also include private entities doing research in pursuit for commercial gain (M. Corrales., M. Fenwick, N. Forgò, *New Technology, Big Data and the Law*, Springer, 2017, 36).

[6] Facebook's Data Policy available at https://www.facebook.com/full_data_use_policy states: "We do not share information that personally identifies you with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you".

accessing them [58] and is the owner of all residual rights not explicitly assigned away to other parties through specific contractual provisions.

It was commented that the individual as a contracting party has less bargaining power than the information industry's company and the option to leave the allocation of the right to the parties will most likely lead to an agreement whereby the latter will retain that right. Hence, some advise introducing laws to overcome such unequal manufacturer market power [58-60].

In a previous work, I tried to resume the current debate on this stance, which may be somewhat simplistically linked back to a trade-off between a property rights model and a contractual approach [61].

In this work, I would like to show that between those extremes a range of possible approaches has been proposed.

7. The "Full- Property Approach"

Economists are generally inclined to think that well-specified property rights are an efficient way to organize an economy since they reduce transaction costs and uncertainty and thereby increase the efficiency of markets.

If the market works well in enabling transactions in other commodities, covered by property rights, it would presumably work for transactions in data as well [62]. Just like with first labour (Locke) or occupancy (Pufendorf), those who *first* collect the data, or generate derivative data from a primary data sets are best entitled to keep their possession, because without them the data would not be existent in the IoT environments. Under this interpretation, all data seem to be explicable and justifiable as belonging to the data collectors because they first do such data collection [50].

Where personal data are involved, propertizing data may also be a way of forcing companies to internalize the costs associated with the collection and processing of data, in the hope that this will lead to greater privacy [63].

Discussing the practical legal modalities of such a right, however, many acknowledge severe theoretical and practical difficulties, starting from the question to whom an ownership right on data should be given [59] [63]. Since data can be copied, multiplied, and mixed with other data and modified, it might be technically very complicated to trace the data transactions, to locate each data and finally say who is the last holder of the data, unless we want to permit data co-ownership.

In any case, the first question that needs to be asked is another. An assumption is widely made that data may be subject to property rights. However, focusing on the issue in terms of "ownership" may be misleading since few jurisdictions treat data as a form of property or simply have different concepts of what property is. Accordingly, the question is whether information is of a tangible or an intangible nature and can be the object of ownership independently from (ownership of) the carrier. In many jurisdictions which follows the model of German law, the object of ownership must be of a physical, i.e. tangible, nature. Consequently, if the "thing" is not physical, as it may be the case with respect to data (seen as an object separate from the carrier), that particular object cannot be "owned" [64].

But even if they were, a main distinction should be drawn between the civil law and common law understanding of ownership [65], which may define the owner's privileges in very different way.

Common law allows private parties more freedom in the types of ownership interests which they can create. Ownership can be dynamic, depending on how large the "bundle of different interests and rights" that it encompasses from time to time [49]. On the other hand, the civil law tradition 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*) [66].

Accordingly, a mistaken assumption that data is property may lead to reliance on statutory provisions which do not in fact, apply. This does not mean that no primary right (in the sense of the maximum of powers, rights, privileges, and immunities) may be designed for data, but rather that it is necessary to be cautious about extending the traditional concept of property to data ownership and whether it would be more accurate to call it "entitlement".

8. The "Semi-Commons" or "Quasi-Ownership Approach"

Some have argued that IPR-like mechanisms are more suitable tools for the purpose of governing data. Since data are non-rival and someone else can use the same data without harm to the previous user, data have different economic properties compared to tangible physical goods. The economic characteristics of data markets are thus comparable to markets for intangible intellectual property.

Heverley [67] sees data as subject to ownership regimes similar to copyright, patents, trademarks and trade secrets. The underlying issue in all these regimes is a dynamic relationship between limited exclusive private rights and exceptions for common use or access – a hybrid ownership regime labeled as "semi-commons" or "quasi-property". It has been defined as a category of property-like interests, which consists of "*situations where the law attempts to simulate the functioning of property's exclusionary apparatus through a relational (liability-like) regime*" [68]: it is a "*relational entitlement to exclude specific actors from a resource given a specific event, a given type of behavior, and/or a given relationship between the actors*" [69].

However, any recognition of a new property right as a particular form of regulation of the market needs an economic justification [70]. Intellectual property exists only where there is a public goods problem and people need incentives to invest, "*i.e. to spend time and money in the creation of new works*" [71].

Most authors observe that there is no evidence of an incentive problem regarding the production and analysis of non-personal data and there is no economic justification for the creation of a new system of data ownership based on the incentive argument. For instance, Hugenholtz [72] argued that data are often a by-product of profitable economic activities and do not require additional incentives.

Although exclusive ownership rights should give financial incentives to the data producer and owner, each owner may affect other owners, excluding them from realizing the potential benefits of economies of scope in the aggregation of datasets. The excessive fragmentation of ownership rights leads to under-utilization of data.

In particular, as it is technologically feasible to keep data secret and protect them against copying and leaking to the public, many argue that the creation of a new system of data ownership is not advisable [72], [73]. Moreover, the recognition that all data are produced mostly automatedly by machines and sensors built into machines excludes that data might be considered as intellectual creations covered by copyright law, traditionally linked to human creative work.

8.1 The "trade secret approach"

A form of quasi-property [74], that may combine the above explored "semi-commons" advantages in relation to data is trade secrets. It has been argued that trade secrecy law has a number of default rules that might be useful for governing data-trade [75], [76]. This law has the same goal of data owners in giving firms/individuals control over commercial exploitations of private information and the power to prohibit their unauthorized uses. Therefore, some scholars [77], [46] suggest to adopt default licensing rules evolved by trade secrecy, like the general rule that if the licensor has provided data to another for a particular purpose, license rights are non-transferable unless the licensor grants a right to sublicense, at the same terms as the license imposes and the data cannot be used for other purposes without obtaining permission for the new uses

This mechanism may allow overcoming some issues related to the intrinsic free alienability, typical of property rights and inappropriate for the information economy.

9. From Property towards Data Access Regime

The question remains whether the data producer's right is the proper approach to tackle the problem. The data producer's right seems to be only one option, and indeed one that is situated at the very interventionist end of the regulatory scale. Hence, others suggest that "ownership" of data should be looked at from a different angle: businesses should not focus on acquiring ownership of data, but on gaining and providing access to data, regardless of their source. As the number of sources and data grows, if you can't use one, you jump to another one, so that the variety on offer will make control or ownership in practice more difficult to operate. Hence, we should not focus so much on who "owns" the data, but who can use them, and for what purpose.

Some scholars propose a more targeted and non-waivable data access rights granted to who has a legitimate interest in access the data so as to conduct data analysis. That would specifically react to situations in which a manufacturer would otherwise try to reserve related markets for itself.

Reichman and Samuelson [78] suggest constructing a liability principle-based regime to protect investors against unfair extractions but requiring to license extractions and reuse on Fair, Reasonable and Non-discriminatory («FRAND») terms. The object is to provide a blocking period against appropriation so that the originator can exercise monopoly pricing in this period subject only to public interest limitations. An automatic universal licence should come into effect as soon as the blocking period ends.

The same approach is proposed by the international law firm Bird & Bird, which issued a White Paper [79] suggesting the creation of an ownership right in data, which should be non-exclusive, in order to allow for a shared use of data by different actors.

The new right would have a mandatory data transfer obligation on FRAND terms and conditions, similarly to what is already known in relation to standard-essential patents.

The Max Plank Institute for Innovation and Competition in its Position Statement on the European Commission's Consultation on Building the European Data Economy took inspiration from Article 20 GDPR and suggested to adopt the data portability right as a general regulatory approach to extend beyond cases of use of personal data.

It also promoted further consideration and discussion for answering more concrete questions such as who should be entitled to claim access or whether a data holder should be remunerated for granting access to data and whether the adoption of general legislation on an access right should be preferred to a sector-specific regulations or viceversa [70].

10. Contractual Approach Remains the "King"

Despite these different possibilities to complete the current legal regime, when stakeholders were asked whether they would favour the introduction of data ownership regulations, they opposed them.

Most respondents to the public consultation on Building a European Data Economy do not support regulatory intervention, whether as an ownership-type rights or as licensing obligations [28].

The majority opinion is that contract law can adequately address issues of data ownership, providing for the flexibility needed to suit the precise situation that different businesses propose. Any legislation in this area, instead, is more likely to hinder the movement of data rather than enhance the data economy.

It is generally accepted that freedom of contract should be "king" in this area and this idea has been strengthened after the CJEU's 2015 decision in *Ryanair v PR Aviation*[7], according to which if a database is not protected by the database right, freedom of contract applies, subject to any restrictions imposed by competition laws or national laws.

So far it is unclear whether this will be the definitive answer to the data ownership issue. The Commission's investigations failed to reach a definitive position, but its proposal for introducing a "data producer's right" (i.e. the owner or long-term user of the device) is still far from achieving consent.

The Working Paper on the economics of ownership, access and trade in digital data by the European Commission's Joint Research Centre [29] declares to be unable to offer policy solutions yet to the question whether a better specification of the scope of data ownership rights would improve efficiency and reduce data market failures.

Likewise, the legal study on Ownership and Access to Data prepared for the European Commission DG Communications Networks, Content & Technology by the international law firm Osborn Clark [80] concluded that it may be necessary to wait for a further evolution of the commercial landscape in order properly to formulate what, if any, legislative intervention would be most appropriate.

While policymakers call for more research to bring economics up to speed with this question, the mid-term objective of this document was to analyse and to set out the possible scenarios of data governance, which may be expected in the foreseeable future.

Such scenarios are the result of a path from full property rights towards complete contractual freedom, passing through the quasi-property approach and the liability-like regime typical of intellectual property rights.

---

[7] CJEU, 15 January 2015, C-30/14, *Ryanair v. PR Aviation*, [2015] ECLI:EU:C:2015:10. For a comment, see M. Borghi, S. Karapapa, Contractual Restrictions on Lawful Use of Information: Sole-source Databases Protected by the Back Door?, *European Intellectual Property Rev.*, **37** (8) (2015), 505.

References

[1] N. N.G. de Andrade, Technology and Metaphors: from Cyberspace to Ambient Intelligence, *Observatorio* (OBS) *Journal* **4** (2010), 1.

[2] G. Riva, F. Vatalaro, F. Davide, M. Alcañiz (eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction*, IOS Press, Amsterdam/Oxford, 2005.

[3] E. H. L. Aarts, S. Marzano (eds.), *The New Everyday. Views on Ambient Intelligence*, Rotterdam, 2003.

[4] *Orientations for Workprogramme 2000 and Beyond*, Information Society Technologies Advisory Group (ISTAG), 1999.

[5] N. Gershenfeld, R. Krikorian, D. Cohen, The Internet of Things, *Scientific American* **291**(4) (2004), 76-81.

[6] A. Greenfield, *Everyware: the dawning age of ubiquitous computing,* New Riders, 2006.

[7] M. Weiser, The Computer in the 21st Century, *Scientific American* **265**(3) (1991), 94-104.

[8] E. F. Adelstein, S. K.S. Gupta, G. G. Richard III, L. Schwiebert, *Fundamentals of mobile and pervasive computing,* McGraw-Hill, 2005.

[9] K. Manwaring, R. Clarke, Surfing the Third Wave of Computing - Contracting with eObjects, *Computer Law & Security Review* **31**(5) (2015), 586-603.

[10] A. Rouvroy, Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, *Studies in Ethics, Law, and Technology* **2**(1) (2008), 51.

[11] G. T. Marx, Technology and Social Control, in N. Smalser, P. Baltes (eds.), *International Encyclopedia of the social and behavioral Science*, Elsevier, Oxford, 2001.

[12] U. Pagallo, M. Durante, S. Monteleone, What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT, in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds.), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Law, Governance and Technology Series **36**, Springer 2017, 59-80.

[13] M. Durante, What is the Model of Trust for Multi-agent Systems? Whether or Not E-Trust Applies to Autonomous Agents, *Know Techn. Pol.* **23** (2010), 347-366; Id., What Model of Trust for Networked Cooperation? Online Social Trust in the Production of Common Goods (Knowledge Sharing), in T.W. Bynum, M. Calzarossa, I. De Lotto, S. Rogerson (eds.), *Living, working and learning beyond technology. Proceedings of the Tenth International Conference Ethicomp 2008*, Mantova, 2008, 211–223.

[14] S. Monteleone, Ambient Intelligence and the Right to Privacy: The Challenge of Detection Technologies, *EUI Working Paper Law* **13** (2011).

[15] D. Lyon, E. Zureik, *Computer, Surveillance and privacy*, University of Minnesota Press, 1996.

[16] U. Pagallo, M. Durante, The Pros and Cons of Legal Automation and its Governance, *European Journal of Risk Regulation*, 7(2) (2016), 323-334.

[17] D. J. Cook., J. C. Augusto, V. R. Jakkula, Ambient Intelligence: Technologies, applications and opportunities, *Pervasive and Mobile Computing*, **5**(4) (2009), 277-298.

[18] N. N. G. de Andrade, Future Trends in the Regulation of Personal Identity and Legal Personification in the Context of Ambient Intelligence Environments: The Right to Multiple Identities and the Rise of the 'AIvatars', in S. Muller, S. Zouridis, M. Frishman, L. Kistemaker (eds.), *The Law of the Future and the Future of Law*, Torkel Opsahl Academic EPublisher, Oslo, 2011, 567.

[19] T. Nabeth, Identity of identity, in K. Rannenberg, D. Royer, A. Deuker (eds.), *The Future of Identity in the Information Society: Challenges and Opportunities*, Springer, Berlin/London, 2009, 53.

[20] K. Rannenberg, D. Royer, A. Deuker (eds.), *The Future of Identity in the Information Society: Challenges and Opportunities*, Springer, Berlin/London, 2009, 23.

[21] R. Clark, The Digital Persona and its application to data surveillance, *The Information Society* **10**(2) (1994), 77-92.

[22] L. Floridi, A Look into the future Impact of ICT on our lives, *The Information Society* **23**(1) 2007, 59-64.

[23] Organisation for Economic Co-operation and Development (OECD), *Data-Driven Innovation. Big Data for Growth and Well-Being*, 2015, 195-196.

[24] World Economic Forum (WEF), *Personal Data: The Emergence of a New Assett Class*, 2011, 7.

[25] EU Commission, *Communication Towards a thriving data-driven economy*, COM(2014) 442 final.

[26] EU Commission, *Communication Building a European Data Economy*, COM (2017) 9 final.

[27] EU Commission, *Staff Working Document On the free flow of data and emerging issues of the European data economy*, SWD (2017) 2.

[28] EU Commission, *Summary report of the public consultation on Building a European Data Economy*, 2017.

[29] N. Duch-Brown, B. Martens, F. Mueller-Langer, JRC Technical Reports on The economics of ownership, access and trade in digital data, *Digital Economy Working Paper* **10**, 2016.
[30] U. Pagallo, The Trouble with Digital Copies: a short KM Phenomenology, in G.J. Morais da Costa, *Ethical Issues and Social Dilemmas in Knowlegde Management: Organizational Innovation*, Information Science Reference, Hershey/New York, 2011, 97.
[31] M. Weiser, J. Seely Brown, The Coming Age of Calm Technology, in P. J. Denning, R. M. Metcalfe, *Beyond Calculation. The Next Fifty Years of Computing*, Springer, New York, 1997, 75-85
[32] D. Tennenhouse, Proactive Computing, *Communications of the ACM* **43** (2000), 43–50.
[33] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, A. Hung Byers, *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute Report, 2011.
[34] Oddenino A., Reflections on Big Data and International Law, *Diritto del Commercio Internazionale* **4** (2017), 777-806
[35] U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, From Data Mining to Knowledge Discovery in Databases, *AI Magazine* **17**(3) (1996).
[36] T. Z. Zarsky, "Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion, *Yale Journal of Law & Technology* **5**(4) (2002), 17–47.
[37] B. Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004, 56-58.
[38] M. Hildebrandt, Profiling and the rule of law, IDIS **1**(1) (2008), 55-70.
[39] U. Pagallo, The Group, the Private, and the Individual: A New Level of Data Protection?, in L. Taylor, L. Floridi, B. van der Sloot (eds.), *Group Privacy. New Challenges of Data Technologies*, Springer, 2017, 159-173.
[40] A. Bonatti, D. Bergemann, Markets for data, *Society for Economics Dynamics Meeting Papers* **538** (2012).
[41] E. Ramirez, J. Brill, M.K. Ohlhausen, J.D. Wright, T. McSweeny, *Data brokers: A call for transparency and accountability*, Federal Trade Commission (FTC), Washington, DC, 2014.
[42] European Data Protection Supervisor (EDPS), *Opinion on Personal Information Management Systems* 9/2016.
[43] IDC, Open evidence, *European data market Final Report*, SMART 2013/0063, 2017, 139.
[44] C. Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, in L. Guibault, P.B. Hugenholtz (eds.), *The Future of the Public Domain*, Kluwer Law International, 2006, 223–257.
[45] J. M. Victor, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data privacy, *Yale L. J.* **123** (2013), 513, 518-519.
[46] G. Malgieri, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, *Journal of Internet Law* **20**(5) (2016), 2-17.
[47] P. Samuelson, Information as Property: Do Ruckelshaus And Carpenter Signal A Changing Direction In Intellectual Property Law?, *Cath. U.L. Rev.* **38** (1989), 365.
[48] S. G. Davies, Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in P.E. Agre, M. Rotenberg (eds.), *Technology & Privacy: The New Landscape*, MIT Press, Cambridge Mass., 1997, 125.
[49] P. Schwartz, Property, Privacy and Personal Data, *Harv. L. Rev.* **117** (2004), 2055, 2060- 2070.
[50] J. Václav, Ownership of Personal Data in the Internet of Things, *Computer Law & Security Review* (2018).
[51] N. Purtova, Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency, Journal of Law and Economic Regulation **10**(2) 2017.
[52] D. Wright, S. Gutwirth, M. Friedenwald, P. De Hert, M. Langheinrich, A. Moscibroda, Privacy, trust and policy-making: challenges and responses, *Computer Law and Security Review* **25**(1) (2009), 69-83.
[53] U. Pagallo, The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection, *Eur. Data Prot. L. Rev.* **3**(1)(2017), 36.
[54] A. Roth, C. Work, *The Algorithmic Foundations of Differential Privacy, Foundation and Trends in Theoretical Computer Science*, **9**(3-4) (2014), 211-407.
[55] A. Chin, A. Klinefelter, Differential Privacy as a Response to the Reidentification Threat: the Facebook Advertiser Case Study, *North Carolina Law Rev.* **90** (2012), 1418.
[56] S. van Erp, B. Akkermans, European Union Property Law, in C. Twigg-Flesner (ed.), *The Cambridge Companion to European Union Private Law,* Cambridge University Press, 2010, 173.
[57] N. Purtova, The Illusion of Personal Data as No One's Property, *Law, Innovation and Technology* 7(1) (2015), 83.
[58] J. Ciani, A competition law oriented look at the application of data protection and IP law to the Internet of Things: towards a wider «holistic approach», in M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt,

G. Serblyte, *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?*, Springer, shortcoming.
[59] H. Zech, Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers", *Computer und Recht* **31**(3) (2015), 137, 145; Id, A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data, *Journal of Intellectual Property Law & Practice* **11**(6) (2016), 460, 464.
[60] K. Zdanowiecki, Recht an den Daten, in Bräutigam P., Klindt T. (eds.), Digitalisierte Wirtschaft / Industrie 4.0, Noerr LLP (2015), 28.
[61] J. Ciani, Property Rights model v. Contractual Approach: how protecting non-personal data in cyberspace?, *Diritto del commercio internazionale* **31**(4) (2017), 831-854.
[62] R. Cooper Dreyfuss, Information Products: A Challenge to Intellectual Property Theory, *N.Y.U. Int'l L. & Pol.* **20** (1988), 925-927.
[63] A. Wiebe, Protection of industrial data – A new property right for the digital economy?, *Journal of Intellectual Property Law & Practice*, **12**(1) (2016), 62–71; *GRURInt.*, 2016, 882.
[64] F. Olivo, Dati personali e situazioni giuridiche soggettive, *Giust. Civ.* **4** (2002), 157.
[65] M. Graziadei, The structure of property ownership and the common law/civil law divide, in G. Michele, S. Lionel (eds.), *Comparative Property Law: Global Perspectives,* Edward Elgar Publishing, 2017.
[66] S. van Erp, Ownership of Data: The Numerus Clausus of Legal Objects, *Brigham-Kanner Property Rights Conference Journal* **6** (2017), 235.
[67] R. A. Heverly, The Information Semicommons, *Berkeley Tech. L.J.* **18** (2003), 1127.
[68] S. Balganesh, Quasi-Property: Like, but not Quite Property, *U. Penn. Law Rev.* **160** (2012), 1891.
[69] L. H. Scholz, Privacy as Quasi-Property, *Iowa Law Review* **101** (2016), 1113.
[70] J. Drexl, R. M. Hilty, J. Globocnik, F. Greiner, D. Kim, H. Richter, P. R. Slowinski, G. Surblytė, A. Walz, K. Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation on Building the European Data Economy", *Max Planck Institute for Innovation and Competition Research Paper* **8** (2017).
[71] M. A. Lemley, Private Property, *Stanford Law Review* **52** (2000), 1545-1557, 1550.
[72] B. Hugenholtz, Europe's sui generis database right, in S. Frankel, D. Gervais (eds.), *The Internet and the emerging importance of new forms of intellectual property*, Kluwer Law, 2016, 205.
[73] J. Drexl, Designing competitive markets for industrial data: Between propertisation and access, *JIPITEC* **8** (2017), 4.
[74] L. Bently, Trade secrets: 'intellectual property' but not 'property'?, in H.R. Howe, J. Griffiths (eds.), *Concepts of Property in Intellectual Property Law*, Cambridge, 2013.
[75] S.K. Sandeen, Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law, Mich. St. L. Rev. (2006), 667.
[76] B. T. Atkins, Trading Secrets In The Information Age: Can Trade Secret Law Survive The Internet?, U. *Ill. L. Rev.* **4** (1996), 1151, 1194,
[77] P. Samuelson, Privacy as Intellectual Property, *Stan. L. Rev.*, **52** (1999), 1125.
[78] J.H. Reichman, P. Samuelson, Intellectual property rights in data? *Vand L. Rev.* **50** (1997), 49.
[79] B. van Asbroeck, J. Debussche, J. Cesar, *White Paper on "Data Ownership"*, Bird & Bird, 2017.
[80] *Legal study on Ownership and Access to Data*, Osborne Clark LLP, 2016.