eLaw
Working Paper Series

No 2018/009 - ELAW– 24 April 2019

Pricing privacy – the right to know the value of your personal data

Gianclaudio Malgieri and Bart Custers

Universiteit Leiden
eLaw

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Pricing privacy – the right to know the value of your personal data

Gianclaudio Malgieri [a,*], *Bart Custers* [b]

[a] *Law, Science, Technology and Society studies (LSTS), Vrije Universiteit Brussel, Belgium*
[b] *eLaw, Center for Law and Digital Technologies, Faculty of Law, Leiden University, The Netherlands*

Keywords:
Privacy
Personal data
Data subject rights
Big data
Digital identities
Data economy

A B S T R A C T

The commodification of digital identities is an emerging reality in the data-driven economy. Personal data of individuals represent monetary value in the data-driven economy and are often considered a counter performance for "free" digital services or for discounts for online products and services. Furthermore, customer data and profiling algorithms are already considered a business asset and protected through trade secrets. At the same time, individuals do not seem to be fully aware of the monetary value of their personal data and tend to underestimate their economic power within the data-driven economy and to passively succumb to the propertization of their digital identity. An effort that can increase awareness of consumers/users on their own personal information could be making them aware of the monetary value of their personal data. In other words, if individuals are shown the "price" of their personal data, they can acquire higher awareness about their power in the digital market and thus be effectively empowered for the protection of their information privacy. This paper analyzes whether consumers/users should have a right to know the value of their personal data. After analyzing how EU legislation is already developing in the direction of propertization and monetization of personal data, different models for quantifying the value of personal data are investigated. These models are discussed, not to determine the actual prices of personal data, but to show that the monetary value of personal data can be quantified, a *conditio-sine-qua-non* for the right to know the value of your personal data. Next, active choice models, in which users are offered the option to pay for online services, either with their personal data or with money, are discussed. It is concluded, however, that these models are incompatible with EU data protection law. Finally, practical, moral and cognitive problems of pricing privacy are discussed as an introduction to further research. We conclude that such research is needed to see to which extent these problems can be solved or mitigated. Only then, it can be determined whether the benefits of introducing a right to know the value of your personal data outweigh the problems and hurdles related to it.

* Corresponding author. Law, Science, Technology and Society studies (LSTS), Vrije Universiteit Brussel, Room 4B 317, Pleinlaan 2, 1050 Brussels, Belgium.
E-mail address: gianclaudio.malgieri@vub.ac.be (G. Malgieri).

https://doi.org/10.1016/j.clsr.2017.08.006
0267-3649/

1. Introduction: from passive defence to active empowerment

The commodification of digital identities is an emerging reality in the data-driven economy.[1] Personal data of individuals represent monetary value in the data-driven economy and are often considered as a counter performance for "free" digital services or for discounts for online products and services.[2] A recent proposal for an EU directive on the supply of digital content has acknowledged that personal data in the modern digital economy can be used, instead of money, to pay for digital content.[3] At the same time, customer data and profiling algorithms are already considered a business asset and protected through trade secrets.[4] However, problematic in this context is that individuals are not often aware of the monetary value of their personal data and tend to underestimate their economic power within the data market and to passively succumb to commodification of their digital identity.[5]

Awareness of individuals is a core element in the big data era and the data-driven economy: it is the optimal balancing between fostering innovation (through the free flow of data) and protecting individuals' human rights. Privacy and personal data protection has often been declined as a *passive defence* of individuals from collection, use and reuse of their data.[6] However, in the big data era, this seems to be both unrealistic and ineffective, because the limiting access and use of data is difficult to enforce and limits the opportunities that big data has to offer.[7] Instead, a more realistic and effective approach towards effective protection of data subjects' interests would be an *active empowerment* of individuals in their personal data management.

An effort that can increase the awareness of and the control over their own personal information could be making consumers/users aware of the monetary value of their personal data.[8] In other words, if individuals are shown the "price" of their personal data, they can acquire higher awareness about their power in the digital market and thus be effectively empowered for the protection of their information privacy.[9]

This is possible by several means. From a theoretical perspective, several solutions have been proposed to make individuals the active players in the data economy, e.g. by forms of "quasi-property" of individuals on their own data.[10] From a more practical perspective, empowering individuals would mean enhancing controllership and awareness of data subjects in the data market. *De lege lata*, this is possible on the one hand through a full exercise of control rights (such as the right to data access, the right to rectification, the right to data portability, the right to be forgotten and the right to block the processing) and on the other hand through the right to receive appropriate information about data processing. While controllership might be enhanced through quasi-propertization theories,[11] increasing awareness of data subjects in the digital market is still an open issue. An effort to address this challenge could be making data subjects aware of the monetary value of their personal data.[12]

The traditional, passive approach to informational privacy has only protected data as per their personal/emotional (qualitative) value. In order to reduce information asymmetry in the big data era and to make individuals stronger players in this data-driven economy, what is necessary is to provide more and more information about the monetary (quantitative) value, i.e., the quantum of their personal data value. This may better indicate the power that individuals really have or can have. It has been shown that if individuals were shown the price of their personal data, their awareness about data processing implications would strongly increase.[13] In this paper we propose – *de lege ferenda* – to introduce a new right of data subjects to receive from data controllers (or an obligation for data controllers to provide to data subjects) information about the monetary value of their personal data.

Firstly, it is analyzed how different types of business models trade personal data in the data-driven economy. These business models can be categorized according to their incentive structures (i.e., monetary and non-monetary) and types of use

[1] Corien Prins, *The Propertization of Personal Data and Identities* (2004), EJCL, www.ejcl.org/83/art83-1.html (accessed 12 June 2017). Nadhezda Purtova, *The Illusion of Personal Data as No One's Property* (2015), Law, Innovation and Technology, vol. 7, n. 1, 2015.

[2] See Wolfie Christl and Sarah Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (Facultas Verlags – und Buchhandels AG, 2016), 65–67.

[3] See Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final, Article 3 (1).

[4] Brenda Reddix-Smalls, 'Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market', (2011) 12 U.C. Davis Bus. L.J. 87, 117-18.

[5] Frederik Z. Borgesius., *Behavioural Sciences And The Regulation Of Privacy On The Internet* (2014), Amsterdam Law School Legal Studies Research Paper No. 2014-54.

[6] World Economic Forum, *Rethinking Personal Data: Strengthening Trust* (2012), http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (Accessed 9 June 2017), p. 9.

[7] Bart H.M. Custers, 'Click here to consent forever; Expiry dates for informed consent', (2016), *Big Data & Society*, 1–6.

[8] See, e.g., Arslan Aziz and Rahul Telang, 'What Is a Digital Cookie Worth?' (March 31, 2016). Available at SSRN: https://ssrn.com/abstract=2757325 (accessed 12 June 2017).

[9] Richard G. Newell, Juha V. & Siikamäki, 'Nudging Energy Efficiency Behaviour: The Role of Information Labels', (2014) 1 J. Association Environmental & Resource Economists 555, 593; Cristiano Codagnone, Francesco Bogliacino and Giuseppe Veltri, *Testing CO2/Car labelling options and consumer information, Final Report* (2013), available at http://ec.europa.eu/clima/policies/transport/vehicles/labelling/studies_en.htm at 9.

[10] Gianclaudio Malgieri, 'Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?', (2016) Journal of Internet Law, Vol. 20, n.5, 2 ff.

[11] See Nadya Purtova, *Property Rights in Personal Data. A European Perspective* (2011) Kluwer International.

[12] See, e.g., Arslan Aziz and Rahul Telang, 'What Is a Digital Cookie Worth?' (2016). Available at SSRN: https://ssrn.com/abstract=2757325 (accessed 12 June 2017).

[13] Richard G. Newell, Juha V. & Siikamäki, 'Nudging Energy Efficiency Behaviour: The Role of Information Labels', (2014) 1 J. Association Environmental & Resource Economists 555, 593, Cristiano Codagnone, Francesco Bogliacino and Giuseppe Veltri, *Testing CO2/Car labelling options and consumer information, Final Report* (2013), available at http://ec.europa.eu/clima/policies/transport/vehicles/labelling/studies_en.htm (accessed 12 June 2017), at 9.

cases (i.e., providing online content, online services or offline services). Also, it is analyzed how EU legislation is already developing in the direction of propertization and monetization of personal data.

Secondly, objective parameters for (estimate) pricing of data are examined, since providing data subjects with a right to know the value of their personal data is only feasible if it is actually possible to quantify the value of these personal data. Different pricing models are discussed, not to determine the actual prices of personal data, but to show that the monetary value of personal data can be quantified, a *conditio-sine-qua-non* for the right to know the value of your personal data. Objective parameters for pricing personal data are established via two methods: a top-down and a bottom-up approach. The first approach corresponds to the supply of digital data, while the second one corresponds to the demand of digital data. The top-down approach corresponds to the demand for digital data and an objective parameter can be found in the price that companies generally pay for personal data of individuals. There are already several studies on this subject, which are based on the businesses' turnover derived from personalized advertisements.[14] The bottom-up approach corresponds to the supply of digital data and is based on a "reverse liability" paradigm,[15] i.e., measuring the value of personal data in terms of damage to privacy or loss of privacy[16] and also in terms of increase of consumer asymmetry.

Thirdly, it is necessary to find a practical way in which this explicit pricing of personal data can be introduced in the digital market. It has already been proposed as a solution to provide an *active choice* to data subjects:[17] when individuals register for a service, they might be asked if they want to pay with money or with their personal data (and with this, they usually accept that data controllers use algorithms to profile their personality). It will be shown, however, that these active choice models are not compatible with the new EU data protection legislation (the General Data Protection Regulation). Article 7(4) states that when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. In other words, it is not possible for service providers to deny the provision of a digital service after the consent to personal data processing that is not necessary for performing the contract has been withdrawn. Indeed, if customers accept to "pay by data" and later withdraw their consent regarding the processing of *unnecessary* personal data, they cannot be denied the provision of the digital service. As a result, service providers and data controllers may end up without payment for their services.

That is why a new data subject right or data controllers "information duty" is the only legal option compatible with the EU privacy approach. What we propose here is an alternative solution: the addition of a new specific obligation to the "information duties" (e.g., under article 13 of the EU General Data Protection Regulation). In all forms of data processing in which the value of data subject's personal data is relevant for the economic transaction, the price of these data (calculated on objective parameters) should be communicated to the data subject. Such a disruptive proposal may increase the shift from privacy as a passive protection, to privacy as an active empowerment of individuals and may, as such, enhance the protection of the right to data protection that each individual has under Article 8 of the EU Charter of Fundamental Rights.

It is obvious that this proposed right to know the value of your personal data also entails several practical problems. These include choosing a pricing method, issues regarding control and consent and issues regarding governance and enforcement. There are also moral problems such as the commodification of inalienable and non-negotiable human rights and the potential reinforcement of existing disparities in society. Then there are cognitive problems such as not taking notice of the pressure to provide information, not understanding such information and the fact that people may not change their behaviour even when they are properly informed. For instance, data subjects having a lower propensity to consume and presumably lower incomes have less valuable data than other consumers have[18] and could have worse contractual conditions.[19] We recognize that some of these problems are significant and provide some preliminary suggestions to mitigate them. Nevertheless, we conclude that further research is needed to see to which extent these problems can be solved or mitigated. Only then, can it be determined whether the benefits of introducing a right to know the value of your personal data outweigh the problems and hurdles related to it.

This paper is structured as follows. Section 2 investigates different types of business models that trade personal data in the data-driven economy and analyzes how EU legislation is already developing in the direction of propertization and monetization of personal data. Section 3 investigates how the value of personal data can be quantified. It is not tried to determine the actual prices of personal data, but to show that the monetary value of personal data can be quantified. Section 4 examines why active choice models are not a viable alternative

[14] John Rose, Olaf Rehse, and Björn Röber, *The value of our digital identity* (2016, New York: The Boston Consulting Group). See also Arslan Aziz and Rahul Telang, 'What Is a Digital Cookie Worth?', op.cit.

[15] Guido Calabresi and A. Douglas Melamed, 'Property Rules, Liability Rules, and Inalienability: One View of the Cathedral' (1972), Faculty Scholarship Series, Paper 1983, 1116 as rephrased (in the field of personal data) by Gintare Surblyte, 'Data as Digital Resource', (2016). Max Planck Institute for Innovation & Competition Research Paper No. 16-12, 37.

[16] Daniel J. Solove, and Danielle K. Citron, 'Risk and Anxiety: A Theory of Data Breach Harms' (forthcoming 2017) 96 Texas Law Review.

[17] Bilyana Petkova and Philipp Hacker, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers' (2016), Lecturer and Other Affiliate Scholarship Series. Paper 13.

[18] Emily Steel, Callum Locke, Emily Cadman and Ben Freese, 'How much is your personal data worth?', Financial Times, (12 June 2013), available at http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz2z2agBB6R (accessed 12 June 2017). see also Emily Steele, *Financial worth of data comes in at under a penny a piece*, Financial Times, June 12, 2013.

[19] Lauren Henry Scholz, 'Algorithmic Contracts' (2016), Stanford Technology Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2747701 (accessed 12 June 2017).

to empower people, as this is incompatible with EU data protection law. Section 5 examines practical and moral problems that the right to know the value of your personal data may rise. Suggestions are made on how to mitigate these problems. Section 6 provides conclusions.

2. De facto monetisation of personal data already at stake

The monetization of personal data is already a reality in nearly all fields of the digital market. The European Commission has highlighted that the market for consumers' data is growing fast and business models based on monetizing data become predominant[20] and a large share of consumers' access digital services offered in return for their personal data. This is the case for around 30% of antivirus and navigation software and cloud storage services, 77% of streamed events and more than 50% of movies, film, TV content, e-books and games.[21] Ensuring an adequate level of protection for these consumers would increase overall consumers' confidence.[22] The economic advantage for customers is balanced by the value of personal profiling which they usually allow by disclosing their personal data. In more technical terms, we can enlist at least three use cases:

a. the "free" or discounted provision of online services,
b. the "free" or discounted provision of (valuable) online content
c. and a "free" or discounted provision of an "offline" service (e.g., insurance, mortgage).

Regarding the first type of use cases, "free" online services, some relevant examples are "free" Wi-Fi services in public spaces, for instance, in airports, when users need to accept cookies and trackers and give their email address if they want to navigate on the Internet. In other words, if they want a free provision of Internet data, they must disclose to the provider (and often to provider's partners) a chronology of websites visited, queries, mailing address, location data, etc. and thus accept a personal profiling.[23] Similar considerations can be made for free cloud services or social networks. A typical example of the second type of use cases are music platforms, like Spotify, where users can access nearly all kind of songs or music pieces at high quality, even if protected by copyright, for free. Customers are asked to create a social profile and to authorize Spotify access to their profile data on Facebook. An example of the third type of use cases is the discount in life insurance policies when using of health trackers. In 2015, John Hancock, one of the largest life insurers in the U.S., teamed up with Vitality, a corporate wellness provider, to offer policyholders a discount when they let a free Fitbit device track their activities. Consumers receive personalized health goals and can log their activities using online and automated tools. By gaining so-called "Vitality Points", they can get a discount of up to 15% on their life insurance policy.[24]

The classification of "free" or discounted provision of digital services, digital content or offline services can also be observed under a different perspective.[25] In strictly economical terms, the transaction between a consumer and a company where there is a mutual exchange of products or services and information is called a "composite transaction" and is different from an "information transaction" when there is a mere flow of information from the consumer to the company. Composite transactions are based on two different steps: the company offers services or products and the consumer purchases them. When the company offers services or products, it also provides information regarding these goods or services and regarding the transaction. At the same time, when the consumer purchases the service or product, he or she can "pay" in different manners. Usually in the digital market, it is possible to pay with money, with (personal) information, or both. This is sometimes referred to as "*disclosure as by-product*".[26]

Since the disclosure of data is an additional element of the traditional exchange of products or services for money, in terms of business models, these business-to-consumer transactions can be classified as follows:

3. Monetary incentives for disclosure as by-product

3.1. *Savings*

Consumers are encouraged to disclose their personal data by a discount covering a part or the totality of the price.

3.2. *Earnings*

Consumers are encouraged to disclose their personal data via a monetary benefit (e.g. a digital wallet).[27] There are in particular

[20] Commission Staff Working Document, Impact Assessment Accompanying the document Proposals for Directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final.

[21] *Ibid*.

[22] *Ibid*.

[23] See, e.g., Ningning Chen, Xinlei Oscar Wang, Prasant Mohapatra, Aruna Seneviratne, 'Characterizing privacy leakage of public WiFi networks for users on travel Conference Paper' in *Proceedings IEEE INFOCOM* (2013).

[24] Wolfie Christl, Sarah Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (Facultas Verlags- und Buchhandels AG, 2016), 66–67 and 290. See also John Hancock (2015): 'John Hancock Introduces a Whole New Approach to Life Insurance in the U.S. that Rewards Customers for Healthy Living' (April 8, 2015), http://www.johnhancock.com/about/news_details.php?fn=apr0815-text&yr=2015, (accessed 12 June 2017). See also for more detalis on the Fitbit program: http://www.thevitalitygroup.com/john-hancock-enters-exclusive-partnership-with-vitality (accessed 12 June 2017).

[25] see Nicola Jentzsch, *State-of-the-Art of the Economics of Cyber-Security and Privacy, IPACSO – Innovation Framework for ICT Security Deliverable*, No. 4.1 (2016), § 3.2.1.

[26] Nicola Jentzsch, Andreas Harasser, Sören Preibusch, *Monetising Privacy – An Economic Model of the Pricing of Personal Information, ENISA Report*, (2012) Greece, www.enisa.europa.eu/activities/identity (accessed 12 June 2017).

[27] This classification is only partially taken from Nicola Jentzsch, *The-state-of-the-Art*, (2016), op.cit. § 3.2.1, Table 8. Actually that clas-

Table 1 – Examples of companies using different business models based on different transaction structures and different use cases.

Incentives / Provision	Monetary		Non-monetary	
	Savings	Earnings	Personalization	No incentives
Digital Content	Spotify		Spotify	iTunes
Digital Service	Wi-Fi in public spaces, Antivirus	Brave	Google, Facebook	Groupon
Offline Service	Hancock insurance	Handshake	Experian	Traditional insurance, etc.

two companies who provide "digital wallets" for the disclosure of personal data: *Handshake* and *Brave*. The former is a platform for finding a job where disclosing personal data can turn into money.[28] The latter is a browser, which blocks all online ads, except those from known advertisers that have accepted to share a part of their income with data users; accordingly, users can earn digital money that they can only spend on financing their favourite content provider.[29]

4. Non-monetary incentives for disclosure as by-product

4.1. *A counter-service*

In particular *personalization*: consumers are encouraged to disclose their personal data by a more tailored service, e.g., a personalized search engine or a personalized social network platform. In some cases, the online services offered may lose some functionality when they cannot be personalized.

4.2. *No incentives*

None of the above incentives applies. In these cases, often consumers have an all-or-nothing choice when disclosing their personal data.

Combining this transaction structure classification with the different types of use cases mentioned above yields different business models. Table 1 shows examples of companies using these different types of business models.

4.3. *Monetization of data in EU legislation*

EU legislation is increasingly taking into account the reality described above. A typical example is the proposed EU directive on "certain aspects concerning contracts for the supply of digital content".[30] With regard to the provision of valuable online content for free, the scope of this proposed directive is restricted in Article 3(1) to any contract where the supplier provides digital content to the consumer or undertakes to do so and, *in exchange*, a *price* is to be paid *or the consumer actively provides counter-performance other than money in the form of personal data or any other data*". Recital 13 remarks indeed that:

> *In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money, i.e., by giving access to personal data or other data. Those specific business models apply in different forms in a considerable part of the market.*

The choice to consider also "free" services "paid by data" within the scope of the proposed directive is due to many factors. First, introducing a differentiation depending on the nature of the counter-performance would discriminate between different business models providing an unjustified incentive for businesses to move towards offering digital content against data. In addition, "defects of the performance features of the digital content supplied against counter-performance other than money may have an impact on the economic interests of consumers". In other words, a narrow scope would not ensure a high level and future-proof consumer protection.[31] In addition, the impact assessment underlines that the strongest impact of rules covering digital content provided in exchange for personal data will be increasing consumers' awareness of the economic value of their personal data and further contribute to better protection.

Recital 14 clarifies also that Directive shall apply only when the customer actively supplies the data (so excluding the case in which the customer accepts cookies), which are not necessary for the digital content to function in conformity with the contract. According to the principle of data minimization (see Article 5(1)(c), GDPR) personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In other words, unless paying with sources "other than money" is part of the declared (and legitimate) purpose, any form of processing of data that are unnecessary for the execution of a contract might be a violation of data minimization principle. The impact assessment of the proposed directive clarifies that the extended scope is consistent with the existing personal data protection framework, which recognises the high importance and value of personal data and that "it does not overlap with data protection rules". However, in order to respect and not overlap

sification does not consider the case of no incentives and classifies differently the monetary incentives, i.e. "earnings" and "payments", where earnings means any economic advantage, while payments means that consumers pays in order to control more their information.

[28] Natasha Lomas, 'Handshake Is A Personal Data Marketplace Where Users Get Paid To Sell Their Own Data', Tech Crunch, (2 September 2013), <https://techcrunch.com/2013/09/02/handshake/> (accessed 28 May 2017).

[29] See <https://brave.com/assets/img/press/brave_infographic_large.png> (accessed 29 may 2017).

[30] COM/2015/0634 final.

[31] See the Impact Assessment, supra.

with data protection rules, the only possibility is that the data controller when collecting data declares the purpose of such data processing and the value the data represents.

Obviously, this is still a proposal and the European Commission mentions also (in its impact assessment) that companies (including those active in the field of digital content development) are against such an extension and advised against overlaps with data protection rules. In particular, some companies argued that the focus should not be on whether the data had been actively provided but rather on how this data is used by the data controllers. For our purposes, we must at least highlight that the EU legislator is starting to acknowledge the de facto monetisation of personal data and is trying to regulate it, though indirectly.

In addition, some digital service providers are starting to admit (perhaps unconsciously) that personal data and user-generated content are a form of payment. A typical example is the End-User Licence Agreement of Instagram, in which Article 1 states that "on Instagram the user provides Instagram with a non-exclusive licence, *totally paid* [for with] the use of content that he or she publishes on Instagram".[32] On Instagram, the registration is free and users do not receive any monetary benefit when they share content (such as images), so the expression "totally paid" seems to refer to non-monetary payment. In other words, according to Instagram's Terms of Use,[33] it seems that users and service providers perform a transaction in which users pay to Instagram for registration, while Instagram pays to users for having a licence on user-generated content. These bilateral payments balance out into a zero-sum and so a "free" digital transaction reveals to be a (implicitly) non-free transaction.

5. Quantifying the value of personal data

When asking how much a person's data is worth, the answer is not much. General information about a person, such as age, gender and location is worth a mere 0.05 cent. Persons who are shopping for a car, a financial product or a vacation are more valuable to companies that want to pitch those goods. For instance, personal data of auto buyers are worth about 0.21 cent per person.[34] Personal data of people going through certain life events, such as becoming a parent, moving, being engaged or getting divorced, also prompt companies to pay more for personal data. For instance, personal data of a pregnant woman are worth about 11 cent.[35] More sensitive personal data are more valuable. Personal data containing specific health conditions or information on taking certain prescriptions are worth about 26 cent per person. However, even adding up all these details means the sum total for most individuals is less than a dollar.[36] However, in principle the data can be sold and resold many times.

It is important to mention that with the development of the data economy, prices of personal data are rapidly going down. For instance, a zip code in the US cost 50 cents in 2006 and 0.05 cents in 2013.[37] This is not only due to lower costs of data collection, but also due to a significant increase in the use of personal data for profiling and marketing.[38] Furthermore, personal data has become ubiquitous, particularly in the United States where personal data can be traded freely, which also drives down prices.

Providing data subjects with a right to know the value of their personal data is only feasible if it is actually possible to quantify the value of these personal data. It is sometimes argued that the value of personal data is intangible, risk-dependent, context-dependent and diffuse.[39] In addition, the underlying values that are at stake, such as privacy, are hard to quantify. For instance, disclosure of personal data may lead to increased risks of future identity theft or fraud, but interpreting such increased risks as actual harm may be too speculative.[40] It might be argued that if it is impossible to quantify the value of personal data, then granting data subjects a right to know the value of their personal data is not realistic.

However, in this section we argue that assessing the value of personal data is not impossible. It is not even that difficult. However, there are some choices to be made, as there exist multiple ways to assess the value of personal data. Attaching a monetary value to personal data requires some clarity on (1) how to express monetary value, (2) which object is actually being priced, and (3) how to attach the value to the object, i.e., the actual pricing system. Hence, in Section 3.1 we start with discussing in which units the value of personal data could or should be expressed. In Section 3.2, we discuss which object is actually being priced and related pricing factors. In Section 3.3, we discuss a number of ways in which the value of personal data can be assessed. These are concrete pricing systems for personal data.

[32] See Instagram Terms of Use, § "Rights", Art. 1, < https://help.instagram.com/478745558852511> accessed 29 May 2017. Italics added.

[33] The deceptive nature of Social media Terms of Use has been however addressed recently in European Commission – Press release, The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules, Brussels, 17 March 2017, < http://europa.eu/rapid/press-release_IP-17-631_en.htm> (accessed 29 May 2017).

[34] Emily Steel, 'Financial worth of data comes in at under a penny a piece', (2013), *op.cit.*

[35] *Ibid.*

[36] The Financial Times has developed a calculator for what a person's personal data is worth. By answering questions on demographics, family & health, property, activities and consumer characteristics, a person can calculate the value of his or her personal data. See: http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4dMtRPoZd (accessed 12 June 2017).

[37] Jay MacDonald, 'How much are your personal details worth?', (21 February 2006), Bankrate.com, http://www.bankrate.com/nsccan/news/pf/20060221b1.asp (accessed 12 June 2017).

[38] More-with-mobile, 'Prices and Value of Consumer Data' (2013) http://www.more-with-mobile.com/2013/06/prices-and-value-of-consumer-data.html (accessed 12 June 2017).

[39] OECD, *Data-driven Innovation for Growth and Well-being, Interim Synthesis Report* (2014).

[40] See, for instance, US case law: Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018 (D. Minn. 2008); Guin v Higher Educ. Serv. Corp. Inc. 2006 WL 288483 (D. Minn. 2006).

5.1. *Expressing value*

Before discussing these pricing systems, it is important to first consider the way in which to express the value of personal data. Intuitively, it would make sense to express the monetary value of personal data in a currency like dollars or euros. However, since personal data are a different product than other, tangible products there are some issues that require further qualifications of this currency based pricing approach.

The first issue is that personal data change over time and may get outdated. For instance, people move and get other addresses. In addition, people may change their interests over time, sometimes gradually (for instance, when they grow older), sometimes immediately (for instance, when they have big life events, like getting married, getting children, facing serious diseases, etc.). As a result, personal data may change and get outdated and, most importantly in this discussion, may lose some of its value. Although we are not suggesting that historical data may not have any value, for purposes like advertising personal data that is up-to-date has the most value. After data (or aggregated datasets) grow older, their value may decrease. Data has to be 'fresh' to be attractive for companies. Hence, it makes sense to argue that personal data is a dynamic product, rather than a static product. Accordingly, it could be argued that the value of personal data may be expressed in terms of euros or dollars *per month*, rather than in euros or dollars. As will be explained below, this also reflects pricing systems that use subscriptions and leases of data rather than selling data.

The second issue is that data, also personal data, can easily be reused.[41] Contrary to tangible products that can only be sold once by a particular owner, data can be copied without additional costs and sold multiple times. Hence, when someone owns personal data, he or she can sell it multiple times. A data subject can sell his or her personal data to different companies. The number of times data can be re-used, determines its value. From the perspective of the data subject, it may be interesting to reuse the same personal data many times to create more value. However, from the perspective of a company that collects personal data, it can only collect personal data from each data subject once. Obviously data collectors can strive for collecting more detailed and complete data on each data subject, each piece of data can only be collected once (unless it has become outdated as explained above). Hence, from the perspective of data collectors it makes sense to express the value of personal data in terms of euros or dollars *per person*, rather than in euros or dollars.

5.2. *Pricing factors*

In the previous section, the term personal data was used in a general way. When raising the question what the value of someone's personal data is, the immediate response is which data? Does this refer to *all* of your personal data or to a specific set, like the personal data on someone's Facebook profile, someone's credit card details or someone's online behaviour and preferences? In this section, we discuss which object is actually being priced when pricing privacy or pricing personal data and related pricing factors.

A first step in this brief analysis is to consider pricing each individual attribute in a personal record. It could be argued that personal data consists of many different attributes of a data subject, often starting with his or her name, address and city of residence. Other common attributes are date of birth, gender, marital status, profession, bank account numbers, etc. Attributes that are more subjective include, for instance, hobbies, interests, and preferences. Some of these attributes may also be objective, when predicted on the basis of big data.[42] Such predictions and statistics may include preferences, life expectancies, credit scores and health risks. We argue that it does not make sense to price the value of each individual attribute in a personal record, as it is the combination of attributes that actually creates value. When the attribute name is provided as 'John' or the attribute gender is provided as 'male', these are meaningless. Single attributes without any further context have no monetary value. Only when combined, i.e., when John is male, these attributes create value.

Hence, pricing personal data is not about pricing individual attributes, but either about pricing attributes of a person or about pricing combinations of attributes. In other words, pricing personal data is about datasets, not about single data, where a datasets starts with combining two data items. In practice, however, many datasets are much larger, increasing the value of personal data. For instance, Axciom, one of the leading US personal data brokers has an average of 1,500 pieces of information on each data subject.[43] It can also be argued that pricing personal data is in fact pricing digital identities, which are the sum of all digitally available information about an individual.[44] These digital identities are becoming increasingly complete and traceable, driven by the exponential growth of available data and technologies to combine and process these data. Pricing digital identities or digital profiles (rather than single attributes) also corresponds better to the practice in which companies that purchase datasets are usually obliged to buy in bulk.[45]

In fact, the *size* of datasets and the *completeness* of datasets are important factors in determining the monetary value of personal data. Knowing that John is male is probably worth less than knowing that John is a male, 35-year old married physician living in a Milwaukee suburb and interested in baseball, jogging and movies. Still, the missing surname of John may affect the value of these personal data negatively. In addition, the *accuracy* and extent to which these data are *up-to-date* affect the monetary value of these personal data. For

[41] Bart H.M. Custers & Helena Ursic, 'Big data and data re-use: a taxonomy of data re-use for balancing big data benefits and personal data protection' (2016), *International Data Privacy Law* 6(1): 4–15.

[42] Bart H.M. Custers, 'Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination', (2012) *Privacy Observatory Magazine* 2012(3).

[43] Paul Boutin, 'The Secretive World of Selling Data about You' (2016), Newsweek, http://www.newsweek.com/secretive-world-selling-data-about-you-464789 (accessed 12 June 2017).

[44] John Rose, Olaf Rehse, and Björn Röber, *The value of our digital identity* (2016, New York: The Boston Consulting Group).

[45] More-with-mobile, 'Prices and Value of Consumer Data' (2013) http://www.more-with-mobile.com/2013/06/prices-and-value-of-consumer-data.html (accessed 12 June 2017).

instance, when these data refer to 1952, they represent a different value then when they refer to 2017. It is important to note that accuracy rates in datasets are often low. For instance, Acxiom, one of the leading US personal data brokers, has estimated accuracy rates of 50 %.[46]

Some data items in a record or profile may be worth more than other data items. For instance, several sensitive characteristics, such as those referring to ethnicity, religion, health, union membership, politics, criminal records, substance abuse and sexual preferences, are more 'telling' about people. Many people also tend to treat these characteristics with more care and disclose them less often. As such, the availability and nature of these characteristics is more *rare* and *unique* and makes them harder to collect. As in general economics, when there is less supply, prices tend to go up.[47]

A final pricing factor is the level of *identifiability* of personal data.[48] Anonymous data does have monetary value, as it may be very useful for several purposes, including policy-making, strategic decision-making and scientific goals. Big data may reveal patterns that are useful for targeted approaches that are not on an individual level. For instance, knowing that diapers and beer cans are usually bought together by customers, especially on Saturdays, is anonymous data that is very useful for targeted marketing and advertising. Nevertheless, knowing the identifying data of the individuals that fall into this category may be worth even more, as it allows an even further personalised marketing and advertising approach.

In summary, when pricing personal data it makes sense to focus on datasets (i.e., digital identities or digital profiles) rather than on pricing individual attributes. Altogether, many factors affect the price of personal data. Factors as size, completeness, accuracy, being up-to-date, rareness and uniqueness, and identifiability can all influence the value. The question is obviously how to add weight to these factors. That, in short, depends on the context and purposes for which the personal data are collected and used. How to determine the actual value of personal data is discussed in the next section.

5.3. *Pricing systems*

There is research available on estimating the value of personal data. A good starting point is OECD survey on methodologies for measuring monetary value of personal data.[49] OECD distinguishes methods that are based on market valuation, and methods that are based on individual's valuation. The market valuation methods focus on (a) financial results for data records, i.e., market cap/revenues/net income per data record, (b) market prices for data, i.e., price per personal data entry offered on the market by data brokers, (c) cost of a data breaches, i.e., economic cost of a data breach (for firms and individuals) per data entry and (d) data prices in illegal markets, i.e., estimation of prices of personal data in illegal markets. The individual's valuation methods focus on (e) surveys and economic experiments, i.e., valuation of personal data in monetary terms that are reported by individuals in surveys or economic experiments and (f) data on willingness of users to pay to protect their data, i.e., amounts that individuals are ready to spend to protect their personal data.

Each of these elements has its drawbacks. As for market-based valuations, the problem is that other factors are often priced-in and several externalities are not considered.[50] For financial results (a), it is highly dependent of the revenues and income of a specific company. For market prices (b), it does not consider the different contexts in which data are demanded. For cost of data breaches (c), there is not any direct proportionality between damages caused by data breach and the actual value of personal data (e.g., damages may include also other factors, like damages to cyber-infrastructures). For illegal markets (d), it does not consider the costs of illegal activities in terms of risks for intruders.[51] All these measures are unilateral and incomplete. Furthermore, they do not consider how much the data are worth for data subjects. However, individual-based valuations (e and f) are also incomplete, because they are not incentive-compatible.[52] Especially for willingness to pay to protect data (f) it has been proven that it does not capture the actual perceived value of personal data.[53]

Petkova and Hacker (2016) have proposed a hybrid methodology, which compares a bottom-up and a top-down approach.[54] The bottom-up approach starts with assessing the value of personal data for advertising. Companies can charge roughly ten times more for personalized advertising than for standard advertising. This difference can be explained by the fact that personalised advertising is a more targeted approach in which no efforts, time and money are wasted on people who are unlikely to respond the advertising anyway. According to industry sources, 1000 personalised advertisements on Facebook mobile would cost approximately 50 cents and about one dollar for the desktop version of Facebook. Hence, each personalized advertisement costs between 0.05 and 0.10 cents.

As discussed in Section 3.1, it may be argued that a price per month makes more sense than a single price expressed in euros or dollars. Assuming that the average user sees about 20 advertisements a day, the revenue from personalized advertising based on personal data for a single data subject is between 1 and 2 cents per day or between 30 and 60 cents per

[46] Paul Boutin, 'The Secretive World of Selling Data about You' (2016), Newsweek, http://www.newsweek.com/secretive-world-selling-data-about-you-464789 (accessed 12 June 2017).

[47] At the same time, the value of redundant data is zero. For instance, when a record shows both someone's age and date of birth, one of these can be used to calculate the other.

[48] See Nicola Jentzsch, *State-of-the-Art of the Economics of Cyber-Security and Privacy*, op.cit., § 3.2.3.2.

[49] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, (2013, OECD Publishing).

[50] Nicola Jentzsch, *State-of-the-Art of the Economics of Cyber-Security and Privacy*, op.cit., § 3.8.1.

[51] *Ibid*. See also OECD, *Exploring the Economics of Personal Data*, op.cit.

[52] Nicola Jentzsch, *State-of-the-Art of the Economics of Cyber-Security and Privacy*, 2016, op.cit., § 3.8.1.

[53] Alessandro Acquisti, Leslie John and George Loewenstein, 'What Is Privacy Worth?', (2013) Journal of Legal Studies: 42 (2)1, http://chicagounbound.uchicago.edu/jls/vol42/iss2/ (accessed 28 May 2017).

[54] Bilyana Petkova and Philipp Hacker, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers', (2016) Yale Law School: Lecturer and Other Affiliate Scholarship Series, paper 13.

month.[55] Obviously, this does not include any further sale, lease or subscriptions to the same data. When this is included, it is likely that the value of personal data will be in the range of 1 to 10 dollars.

The top-down approach estimates the value of personal data with a different calculation strategy, in which the total revenue and the total number of users of a company processing personal data are used as a starting point. For instance, Facebook had total revenue of 17.93 billion dollars in 2015, most of which was revenue from advertising.[56] At the end of 2015, the total number of users was 1.59 billion.[57] Thus, Facebook generates an average of about ten dollars of revenue from advertising per year, which is about one dollar per month. The results of this calculation are in line (same magnitude) with the bottom-up approach.

This approach does not take into account the price at which data subjects would be likely to disclose their own personal data. That is why it may be argued that the loss of privacy is also included in the pricing of personal data. Since individuals tend to under-estimate the effects of disclosing their own personal data and are often unconscious of inferences, Data Protection Authorities can better determine predictions and discrimination that can arise from disclosure.[58] Privacy harms can be either subjective harms (i.e., the distress for data breach)[59] or objective harms (i.e., information asymmetry and discrimination).[60] When individuals disclose their data they suffer an objective loss of privacy in terms of higher exposure to discrimination (including price discrimination) and information asymmetry, which may yield commercial vulnerability. Subjective harms may be difficult to quantify, though this may not be entirely impossible.[61] Objective harms are more straightforward to be quantified by courts or Data Protection Authorities. There is case law available that has monetized privacy damages in terms of discrimination and vulnerability risks.[62] Obviously, these examples of pricing privacy by courts involve cases in which actual violations of privacy rights took place. These pricing methods can be used in the context of the right to know the value of your personal data by applying so-called "reverse liability".[63] This means calculating a compensation that a potential infringer (e.g., a company, a data controller) pays ex ante in order to be allowed to perform a probably harmful activity (e.g., processing personal data).

The wide range of methods discussed in this section shows that monetary value of personal data value can be quantified. The aim of this paper is not to determine the actual prices of personal data, but to show that this important requirement for the right to know the value of your personal data is not an obstacle.

6. "Active choice" models and the GDPR

There are several ways to increasing consumers' awareness about monetisation of personal data in the modern information society. It may be suggested that there are better alternatives for a right to know the value of your personal data. Particularly so-called "active choice" models are often mentioned in this respect.[64] These models refer to an active choice for consumers between paying for a digital service with money (without any consent to the service provider to perform a profiling on the customer data) and accessing the service for free while disclosing personal data, usually allowing personal profiling. In other words, the active choice is between paying by data and paying by money. At the same time, data controllers who provide digital services would have the obligation to provide this active choice to their customers. This approach addresses the problem of unilateral monetisation of personal data in the modern digital economy and it proposes an effective safeguard that might actively increase awareness of data subjects and empower them in the digital market. Indeed, according to the "active choice" model, the flow of data or money in the supply of digital services would depend on individual choices.

However, active choice models have several compatibility problems with the EU legal framework for personal data protection, particularly with regard to the General Data Protection Regulation (GDPR). Article 7(4) of the GDPR, when referring to the assessment of freedom of consent for the processing of personal data, states that:

> *Utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

[55] This is in line with other sources, for instance, More-with-mobile, 'Prices and Value of Consumer Data' (2013) http://www.more-with-mobile.com/2013/06/prices-and-value-of-consumer-data.html (accessed 12 June 2017).

[56] See www.marketwatch.com/investing/stock/fb/financials (accessed 12 June 2017).

[57] See www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide (accessed 12 June 2017).

[58] Bart H.M. Custers, Simone van der Hof S& Bart Schermer, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies', (2014) Policy and Internet 6(3): 268–295.

[59] See Daniel J. Solove & Danielle Keats Citron, 'Risk and Anxiety: A Theory of Data Breach Harms', (2017) GW Law School Public Law and Legal Theory Paper No. 2017-2.

[60] Ryan M. Calo, 'The Boundaries of Privacy Harm' (2011), Indiana Law Journal: Vol. 86: Iss. 3, Article 8.

[61] Daniel J. Solove, and Danielle K. Citron, 'Risk and Anxiety: A Theory of Data Breach Harms' (2017), op.cit.

[62] See, e.g., in the US jurisprudence, *Padilla v. Kentucky*, 130 S. Ct. 1473, 1483 (2010) (requiring component counsel to inform client of potential "adverse immigration consequences"); *Ricci v. DeStefano*, 129 S. Ct. 2658, 2672 (2009) (defining "disparate impact" as having a "disproportionately adverse effect on minorities"); *Safeco Ins. Co. of America v. Burr*, 551 U.S. 47, 62 (2007) (discussing "adverse effects" under the Fair Credit Reporting Act). See a general discussion about it in Ryan M. Calo, 'The Boundaries of Privacy Harm' (2011), op.cit., 1151.

[63] *Reverse liability* is a concept taken from Guido Calabresi and A. Douglas Melamed, 'Property Rules, Liability Rules, and Inalienability: One View of the Cathedral' (1972). Faculty Scholarship Series. Paper 1983, 1116 as rephrased (in the field of personal data) by Gintare Surblyte, 'Data as Digital Resource' (2016), Max Planck Institute for Innovation & Competition Research Paper, No. 16-12, 37.

[64] Bilyana Petkova and Philipp Hacker, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers', (2016), op.cit.

In other words, if a data subject is asked to consent to the processing of personal data (which is not necessary for the performance of that contract) in order to have access to a service or for the performance of a contract, it is highly probable that his consent is not "free", and so it is not valid under the GDPR.[65]

In the active choice model, individuals might "pay by data", i.e., they would be required to consent to authorize access to and processing of personal data that is not necessary for the provision of that service. Once they pay with their data, they cannot withdraw their consent freely: given that personal data would be a "counter-performance other than money", blocking that data processing would mean blocking the provision of that service. However, as recital 42 of GDPR states, the withdrawal of consent must be "without detriment" to the data subject. In sum, it seems that the active choice model is not compatible with the EU data protection legislation. That brings us back to our proposal to introduce a right to know the value of your personal data rather than the right to have an active choice between paying with money or with personal data.

Research has shown that informing consumers about prices is a very effective way to increase attention of consumers while reading pre-contractual information papers and so to increase consumers' awareness.[66] In the GDPR, there are several provisions about the duty to inform data subjects. In particular, articles 13, 14 and 15 provide a list of pieces of information that should be given to data subjects in different situations. The data subject has the right to know (inter alia) the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended, the categories of personal data concerned, the period for which the personal data will be stored, and from which source the personal data originate. If applicable, rights also extend to whether it came from publicly accessible sources, the existence of data subject's rights, the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[67]

Although this is an extensive list of information duties, there is no specific provision referring to the economic value of personal data or personal profiling. Data controllers should inform individuals about the purpose of data processing. If data controllers process personal data as a counter-performance other than money, they should clearly declare that purpose to the data subject, otherwise any processing of personal data, which are not necessary for the declared purpose (e.g., performance of a contract) would be a breach of the data minimization principle and the purpose limitation principle.[68] In other words, any case in which unnecessary[69] personal data is collected as a "counter-performance other than money" for the provision of a service, it must be declared.

Obviously, unnecessary personal data (for instance, via cookies) are often collected via "alternative" purposes, such as improving the provision of a digital service or improving the experience of customers. Although data controllers should declare that personal data, which are not necessary for the performance of a contract are collected as an alternative payment for that service, they do not have any duty to "price" those data or to inform users about these prices. That is why we propose *de lege ferenda* adding a new right to information to article 13 and 14 GDPR: *in each data processing where the value of customers' personal data is relevant for the economic transaction, the price of these data should be communicated to the consumer.*

To further concretize this provision, Data Protection Authorities should be entitled to monitor and enforce this obligation. They could *ex ante* release guidelines about actual prices to be set for personal data, releasing tables for personalization of prices, describing circumstances in which these calculations could vary, ex post monitor, and investigate if data controllers respect these guidelines.

7. Problems of pricing privacy

In this section, we discuss some problems of the idea to introduce the right to know the value of our own personal data in EU data protection law. In Section 5.1 we discuss practical problems, in Section 5.2 we discuss broader moral problems and in Section 5.3 we discuss cognitive problems.

7.1. *Practical problems*

There are several practical problems raised by the implementation of the right to know the value of your personal data. The first problem is that of determining the actual prices. As discussed in Section 3, there are several methods for this. A choice can be made for one of these methods, but each choice may have drawbacks in the ways the calculation reflects the actual value of personal data. In other words, each method for determining prices is simply a reflection, an approximation of the actual value and may sometimes be a close estimate, but at other times significantly wrong. We think this may still work, as choosing a method, even when it occasionally is off mark, is better than nothing.

A second, related practical problem is who should do the pricing. The most obvious choice is to let data controllers do the pricing, as they may have the best knowledge to do this and it lays the burden of this task on the plate of those who profit from the data. Still, it is obvious that data controllers will be reluctant, to say the least, to pick up this task. First, it means yet another obligation to them, in which they have to be compliant and which will involve additional costs, perhaps yielding

[65] See the definition of "consent" at Article 4, GDPR.

[66] Richard G. Newell, Juha V. & Siikamäki, 'Nudging Energy Efficiency Behaviour: The Role of Information Labels', (2014), op.cit.

[67] See article 13(1–2), 14(1–2), 15(1), GDPR.

[68] Article 5(1): "(personal data shall be: "adequate, relevant and limited to what is necessary in relation *to the purposes* for which they are processed" (lett. b) and "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (lett. c).

[69] i.e., not necessary for the performance of the contract at stake between data controller and data subject.

reduced profits. Second, data controllers may fear that their business models will be revealed. When consumers know the value of their personal data, they may also be able to see how much data controllers profit from these data. Although we think this actually constitutes a good reason to provide data subjects with this information, data controllers may argue that this reduces their competitiveness. When the value of personal data for each data controller, specifically data brokers, is transparent, it also reveals how (and how much) money these organisations are making. This reveals their business models and, when copied by competitors, may render them out of business. However, there may also be opportunities for businesses here. Research shows that consumers that experience more control (i.e., who are able to manage and protect their privacy, for instance via privacy settings) are up to 52 % more willing to share information than those who are not.[70]

When deciding that data controllers should do the pricing, it should also be taken into account that they may have something to gain from modifying the prices. When online services are paid with by personal data, it is profitable for data controllers to argue that the personal data has little value. In that way, they will get more personal data for their services. When payments are made with money, prices can be negotiated. When payments are made with personal data, this is no different. However, when the counterparty can first determine how much you money (i.e., your personal data) is worth before negotiating the price, this may be unfair. We think this problem can be addressed by creating objective rules for the pricing system in combination with mandatory transparency and supervision of data protection authorities, but this is something to take care of.

This brings us to the third problem, which is that supervision and enforcement may be complicated. It may be argued that it will be quite different a task than they are used to for Data Protection Authorities to supervise these monetary issues. In response to this, we would argue that Data Protection Authorities would have to focus on legal compliance with this provision to provide information on the value of personal data, which is not very different from other compliance issues in the data protection domain. Supervision would start with verifying whether such information is actually provided. If so, the next step would be to verify whether the information was provided correctly and in an appropriate way. This problem would be similar to checking compliance with other information duties that data controllers have under articles 13 and 14 of the GDPR. Checking whether pricing information was provided correctly is something that can be checked by comparing prices with similar organisations and that can be realised with the investigative and corrective powers that Data Protection Authorities have under articles 31 and 58 of the GDPR. Data Protection Authorities can (ex ante) release appropriate guidelines with specific templates for the calculation of prices (e.g. some schemes, examples and specific proposals) and (ex post) check how data controllers implement such guidelines.

A fourth problem are so-called "privacy externalities".[71] An example of this is that some data may be already made public by data subjects through social networks. Paying with personal data that is available free elsewhere may be a hard business case. However, it should be kept in mind that when data subjects disclose their personal data online, this does not imply consent to use or reuse these data for any given purpose. Further processing or reuse of data is subject to new or additional consent of the data subject. Another example is that, with the development of data retrieval technologies (i.e., data mining, machine learning, profiling)[72] more and more data can be inferred or predicted from fewer and fewer raw personal data.[73] This also changes the value of personal data. A final example is that personal data disclosed by a data subject may reveal data referring to other individuals[74] (e.g., DNA, marital status). Accordingly, it has been argued that personal data of individuals are increasingly shifting towards multiple subjects' personal data, where information is interdependently related to multiple transaction parties.[75] Consequently, it is very difficult for individuals to control this chaotic flow of personal data and difficult for data controllers to set a stable price for them.

At the same time, the value of personal information might change over time. In some cases, personal data might lose its value when time goes on and in other cases, it could acquire more value after a certain period.[76] Solutions for this difficulty to check the value of personal data in complex information chains require further research and are beyond the scope of this paper. As a preliminary example, we observe that blockchain technologies might potentially be applied in the field of personal data value in order to track the flow of data.[77] The

[70] John Rose, Olaf Rehse, and Björn Röber, *The value of our digital identity* (2016, New York: The Boston Consulting Group), p. 13.

[71] Nicola Jentzsch, *The State-of-the-art of Cyber-Security and Privacy*, op.cit., § 3.2.2.2. See also Stefania Gnesi, Ilaria Matteucci, Corrado Moiso, Paolo Mori, Marinella Petrocchi and Michele Vescovi, 'My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data', in B. Preneel and D. Ikonomou (eds.), *Privacy Technologies and Policy, Lecture Notes in Computer Science*, (2014) Vol. 8450, pp. 154–171.

[72] Toon Calders and Bart H.M. Custers, 'What is data mining and how does it work?', in Bart H.M. Custers, Toon Calders, Bart Schermer, Tal Zarsky (eds.) *Discrimination and Privacy in the Information Society* (2013, Springer, nr. 3. Heidelberg).

[73] Michal Kosinskia, David Stillwella, & Thore Graepelb, 'Private traits and attributes are predictable from digital records of human behavior', in *Proceedings of the National Academy of Sciences of the United States of America* (2013), 110(15): 5802–5805.

[74] Nicola Jentzsch, The State-of-the-Art, op.cit., § 3.2.2.2.

[75] Stefania Gnesi, Ilaria Matteucci, Corrado Moiso, Paolo Mori, Marinella Petrocchi and Michele Vescovi, 'My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data, 2014, op.cit., pp. 154–171.

[76] See Gianclaudio Malgieri, Giovanni Comandé, "Sensitive-by-distance: Quasi-health data in the algorithm era" (2017), Information and Communications Technology Law, Issue n. 6, forthcoming.

[77] See, e.g. Fidel Santiago, Multiple Views on Blockchain: Technology, Use Cases, Economics, and Policies, intervention at the EDPS Conference, *Data protection and blockchain technologies*, Brussels,17 June 2016. For innovative uses of Block Chain in the field of information privacy see also, e.g., Bell, Tom W., Copyrights, Privacy, and the Blockchain (2016). Ohio North University Law Review, Vol. 42, 2016; Chapman University, Fowler Law Research Paper No. 16-09. Available at SSRN: https://ssrn.com/abstract=2815717. see, e.g., Malki,

further commodification of personal data may involve micropayments that otherwise involve transaction costs that are too high to implement. However, with the use of blockchain technology, such micropayments can be implemented at low costs.

A final problem is that it may not be clear how and when the pricing information should be provided. Should it be in the privacy policy or in the general terms and conditions, should it be presented when registering for an online service or should it be send to users in period news messages? We would argue that the best approach in terms of transparency would be to use all these sources. However, it does not have to be decided in legislation, we think. The provision of this information can simply follow the reasoning of all the other information duties for data controllers laid down in articles 13 and 14 of the GDPR. These information duties are not phrased in a way that determines where and when such information should be provided.[78] The only requirement is how the information should be provided, which can be found in Article 7, paragraph 2, which states that all such information should be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. This provision can also be applied to information on the value of someone's personal data.

7.2. *Moral problems*

Apart from the practical problems mentioned above, there are also some ethical and moral problems that can be identified when going down this road of pricing privacy.[79] The first problem is that personal data rapidly becomes a commodity that can be traded. Personal data, however, are closely related to the privacy of a data subject. Commodification of privacy may be considered an undesirable approach, as privacy and other human rights are inalienable and non-negotiable. In the US, trading personal data without any legal restrictions is very common, but this is an approach that is frowned upon in the EU. The EU created the GDPR (and preceding legislation) exactly to avoid uncontrolled spreading and use of personal data in order to enable data subjects to protect their personal data. EU legislation specifically empowers data subjects with control rights. Therefore, we argue that commodification of privacy and personal data is not at risk in our proposal to introduce a right to know the value of your personal data. Even when people want to sell away their data privacy, they are unable to do this, from a legal perspective. They will always have several inalienable rights with regard to their personal data, regardless of who is processing them. In addition, they will always have the right to withdraw their consent to such processing.[80] Hence, personal data can be commodified, but personal data rights will still be intact.

A second problem of pricing privacy is that the value of personal data of some people will be worth more than that of others. As was already explained in Section 3, personal data of people who have more to spend (and consequentially higher propensity to consume) will probably be worth more to data controllers. As a result, there may occur something that can be called ex ante discrimination, which personal data of poor people is less valuable and personal data of rich people is more valuable. This may reinforce existing disparities in society.[81] Poorer people are generally more price-sensitive,[82] while richer people are less price-sensitive, but have a higher propensity to consume. When attracting customers, companies may offer larger discounts to interesting (i.e., profitable, rich) customers. As such, rich people may get better prices and poor people may get lousy offers.[83] Actually, this is disputable: there are several more factors influencing price discrimination, e.g. it has been argued that personalization of online commercial offers should work to the benefit of more price-sensitive people, and so there should be lower costs for consumers with fewer resources.[84]

In sum, although data price discrimination might be a serious problem, potentially increasing stigmatization and polarisation in society, there are several more factors and variables that distort its effects, so that pricing digital identities cannot prove to be a discriminatory practice itself. To the contrary, it would be a dynamic tool enhancing awareness and thus information power of data subjects against unfair practices of data controllers. Similarly, we do not think this problem can be solved in data protection legislation alone. It may require stronger legislations in the domains of non-discrimination law, competition law and criminal law.

Amer and Weiss, Martin B. H., Automating Ex-Post Enforcement for Spectrum Sharing: A New Application for Block-Chain Technology (March 31, 2016). Available at SSRN: https://ssrn.com/abstract=2754111 or http://dx.doi.org/10.2139/ssrn.2754111.

[78] See, e.g., Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017), International Data Privacy Law, Forthcoming.

[79] For a general view about moral problems related to "monetization" of personal data see e.g. Nicola Jentzsch, *State-of-the-Art of the Economics of Cyber-Security and Privacy*, *IPACSO – Innovation Framework for ICT Security Deliverable*, (2016) No. 4.1, § 3.7.

[80] Bart H.M. Custers, Simone van der Hof, Bart W. Schermer, Sandra Appleby-Arnold and Noellie Brockdorff, 'Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law' (2013), in *Script-ed: a journal of law and technology* 10(4): 435–457.

[81] Bart H.M. Custers, 'Data Dilemmas in the Information Society', in Bart H.M. Custers, Toon Calders, Bart W. Schermer, Tal Zarsky (ed.) *Discrimination and Privacy in the Information Society* (2013, nr. 3. Heidelberg: Springer).

[82] See, e.g., Andrew Odlyzko, 'Privacy, economics, and price discrimination on the Internet' (2003) Proceedings of the 5th international conference on Electronic commerce (ACM) 355. See also Exec. Office of The President of United States, *Big Data And Differential Pricing*, (2015) 17, http://www.whitehouse.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf (accessed 12 June 2017), p. 17.

[83] See also Cathy O'Neil, *Weapons of Math Destruction; How big data increases inequality and threatens democracy*, (2016, New York: Crown).

[84] See Exec. Office of The President of United States, *Big Data And Differential Pricing*, (2015) 17, http://www.whitehouse.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf (accessed 12 June 2017): "[I]f historically disadvantaged groups are more price-sensitive than the average consumer, profit-maximizing differential pricing should work to their benefit" in competitive markets".

7.3. *Cognitive problems*

Even if individuals are provided with information on the value of their personal data, it does not mean that they will consistently profit from this additional information. In this subsection, we discuss some cognitive issues that may either limit or nullify the effects of a right to know the value of your personal data.

The first cognitive issue is that people may not take notice of the information offered. Research has shown that people largely tend to ignore privacy policies of online services.[85] Offering information on the value of personal data, for instance, via privacy policies or other types of notifications, may suffer from the same flaws that affect other information rights in the GDPR. Only small numbers of people actually read privacy policies and when they do, they only read parts of it. Moreover, if they read this, people may not comprehend the information fully and if they read and understand the information provided, they may still not understand the consequences of the information provided. Finally, even if they understand the consequences, the policies and settings may not offer the options they prefer.[86] This may also apply to providing information on the value of personal data: people may not take notice, may not understand the information provided, may not understand the consequences and may not be able to act upon this information in ways they would like. These are cognitive problems that may limit the extent to which a right to know the value of your personal data actually increases awareness or enables controllership.

At the same time, it may be argued that providing information on the value of personal data may not suffer from all of these flaws: for the tendency to ignore privacy policies, we have already mentioned that "prices" may be an exception, since it has been shown that when consumers read "prices" their reading attention is strongly enhanced.[87] Thus, including "prices" in privacy policies might actually be an incentive to increase the tendency to read privacy policy in general and to take notice of the value of personal data specifically.

Another cognitive problem is that data subjects often suffer social pressure to use certain online tools.[88] In other words, even if there might be valid reasons or incentives (such as better value for your personal data) to quit a digital platform or to change digital services, social pressure caused by the great diffusion of online media (e.g. Facebook, Twitter) might strongly limit users' freedom of choice and persuade them to continue using a specific online tool, regardless of any (social, moral or economic) implications.[89] The consequence is that individuals' information power in the digital market might be highly limited. In such cases, a right to know the value of your personal data may increase awareness, but will not result in effective empowerment and increased controllership of users.

This issue is not limited to the newly proposed right to know the value of your personal data, but includes also the already existing information rights mentioned in Article 13 and 14, GDPR as well as the actual impact of the informed consent, of the right of access, the right to data portability, the right to erasure, etc. A possible way to limit these social pressure issues might be to limit the monopolistic power of social media and digital services through competition law[90] or to through specific regulations.[91] Further research on how to deal with these issues is required, but is beyond the scope of this paper.

8. Conclusions

In this paper, we analysed whether consumers/users should have a right to know the value of their personal data. The main reason to consider this question is because, on the one hand, the commodification of digital identities is an emerging reality in the data-driven economy and, on the other hand, individuals do not seem to be fully aware of the monetary value of their personal data. They tend to underestimate their economic power within the data-driven economy and to passively succumb to the propertization of their digital identity. Introducing a right for data subjects to know the value of their personal data may increase their awareness of their own personal information and about their power in the digital market and thus effectively empower them for the protection of their information privacy.

We have shown that the current data-driven economy de facto already monetizes personal data. A variety of different online business models exist in practice, with different incentives for data subjects to 'pay' with their data. In addition, EU legislation is increasingly taking into account this new reality. Next, we investigated different methods for quantifying the value of personal data, not to determine the actual prices of personal data, but to show that the monetary value of personal data can be quantified, a *conditio-sine-qua-non* for the right to

[85] Acquisti, A. (2009), Nudging Privacy: the Behavioral Economics of Personal Information, in: Security & Privacy Economics, November/December 2009.

[86] Solove, D. J. (2013), Privacy Self-management and the Consent Dilemma, in: Harvard Law Review, vol. 126, pp. 1880–1903.

[87] See supra at section 1. See, e.g., Richard G. Newell, Juha V. & Siikamäki, 'Nudging Energy Efficiency Behaviour: The Role of Information Labels', (2014), op.cit.

[88] See, e.g., Iyengar, Raghuram and Han, Sangman and Gupta, Sunil, Do Friends Influence Purchases in a Social Network? (February 26, 2009), Harvard Business School Marketing Unit Working Paper No. 09–123. See also Rao, Gayathri and Madan, Ankur, "A Study Exploring the Link between Attachment Styles and Social Networking Habits of Adolescents in Urban Bangalore" (May 30, 2012). International Journal of Scientific and Research Publications, Vol. 3, Issue 1, January 2013. See also Kharzraee, Emad and Unsworth, Kristene, Social Media: The New Opiate of the Masses? (December 1, 2012). International Review of Information Ethics, Vol. 18 (12/2012).

[89] See, e.g., Vranaki, Asma A.I., Social Networking Site Regulation: Facebook, Online Behavioral Advertising and Data Protection Laws (February 11, 2016). Queen Mary School of Law Legal Studies Research Paper No. 221/2016, arguing that "the elicitation of valid consent in Facebook can often be a "perfunctory" and banal process which is reduced to mundane actions, such as button clicks. Here, I question to what extent Facebook users can be said to have provided valid consent in accordance with the applicable laws".

[90] See, e.g., Waller, Spencer Weber, Antitrust and Social Networking (October 24, 2011). North Carolina Law Review, 2012. Available at SSRN: https://ssrn.com/abstract=1948690.

[91] See, e.g., Vranaki, Asma A.I., Social Networking Site Regulation: Facebook, Online Behavioral Advertising and Data Protection Laws (February 11, 2016). Queen Mary School of Law Legal Studies Research Paper No. 221/2016,

know the value of your personal data. Furthermore, active choice models, in which users are offered the option to pay for online services, either with their personal data or with money, were examined. However, it was concluded that these models are incompatible with EU data protection law. Hence, these models do not provide a viable alternative to increase awareness and control of data subjects regarding their personal data.

Therefore, a right for data subjects to know the value of their personal data may be a practical and realistic approach to empower data subjects towards this commodification of digital identities. Informing consumers about prices is a very effective way to increase attention of consumers while reading pre-contractual information papers and so to increase consumers' awareness. To some extent, there already is an obligation for data controllers under EU data protection law to inform data subjects when they consider providing personal data as 'payment'. That is, when personal data is collected that is strictly speaking unnecessary for performing the contract, the personal data is collected as a "counter-performance other than money" and must therefore be declared. If not, any such processing of personal data would be a breach of the data minimization principle and the purpose limitation principle.

In articles 13, 14 and 15 the GDPR there are already several provisions about the duty to inform data subjects. It would be quite straightforward to add a new right to information to article 13 and 14 GDPR reading something like: *in each data processing where the value of customers' personal data is relevant for the economic transaction, the price of these data should be communicated to the consumer.* Data Protection Authorities should be entitled to monitor and enforce such an obligation. They could *ex ante* release guidelines about actual prices to be set for personal data, releasing tables for personalization of prices, describing circumstances in which these calculations could vary, ex post monitor, and investigate if data controllers respect these guidelines.

It is obvious that this proposed right to know the value of your personal data also entails several practical problems (such as choosing a pricing method, issues regarding control and consent and issues regarding governance and enforcement). Then there are moral problems (such as the commodification of inalienable and non-negotiable human rights and the potential reinforcement of existing disparities in society) and cognitive problems (such as not taking notice of the information provided pressure, not understanding such information and the fact that people may not change their behaviour even when they are properly informed). We recognize that some of these problems are significant and have provided some preliminary suggestions to mitigate them. Although we think that introducing a right to know the value of your personal data may contribute to increasing awareness, it is much less clear that it will also provide more controllership of consumers/users on their own personal data. We acknowledge that this proposed new information right should only be introduced when individuals can actually apply and uphold it.

That is why we conclude that further research is needed to see to which extent the practical, moral and cognitive problems we identified can be solved or mitigated. Only then, can it be determined whether the benefits of introducing a right to know the value of your personal data outweigh the problems and hurdles related to it. With this agenda-setting paper, we hope to start a discussion on these topics that will pave the way for this new right to know the value of your personal data.

Author information

Gianclaudio Malgieri, LLM is a PhD Researcher at the Law, Science, Technology and Society studies (LSTS) of Vrije Universiteit Brussel, Belgium. Email Address: gianclaudio.malgieri@vub.ac.be. Bart Custers PhD MSc LLM is associate professor and head of research at eLaw, the Center for Law and Digital Technologies at the Faculty of Law of Leiden University, the Netherlands.

REFERENCES

A Acquisti, L John and G Loewenstein, What is privacy worth?, (2013) J Leg Stud: 42 (2)1, http://chicagounbound.uchicago.edu/jls/vol42/iss2/1/. Accessed 28 May 2017.

A Aziz and R Telang, What is a digital cookie worth? 2016. Available from: https://ssrn.com/abstract=2757325. Accessed 12 June 2017.

FZ Borgesius., Behavioural sciences and the regulation of privacy on the internet, 2014. Amsterdam Law School Legal Studies Research Paper No. 2014-54.

P Boutin, The secretive world of selling data about you, newsweek; 2016. Available from: http://www.newsweek.com/secretive-world-selling-data-about-you-464789. Accessed 12 June 2017.

G Calabresi and A Douglas Melamed, Property rules, liability rules, and inalienability: one view of the cathedral, 1972. Faculty Scholarship Series, Paper 1983, 1116

T Calders and BHM Custers, 'What is data mining and how does it work?', in BHM Custers, T Calders, B Schermer, T Zarsky (eds.) Discrimination and privacy in the information society (2013, Springer, nr. 3. Heidelberg).

RM Calo, The boundaries of privacy harm (2011), Indiana Law J: 86: Iss. 3, Article 8. Group, p. 13.

N Chen, XO Wang, P Mohapatra, A Seneviratne, Characterizing privacy leakage of public WiFi networks for users on travel Conference Paper. in Proceedings IEEE INFOCOM, 2013.

W Christl and S Spiekermann, Networks of control: a report on corporate surveillance, digital tracking, big data & privacy. Facultas Verlags – und Buchhandels AG, 2016.

C Codagnone, F Bogliacino and G Veltri, Testing CO2/Car labelling options and consumer information, Final Report; 2013. Available from: https://ec.europa.eu/clima/sites/clima/files/transport/vehicles/labelling/docs/report_car_labelling_en.pdf.

BHM Custers, Predicting data that people refuse to disclose; how data mining predictions challenge informational self-determination, (2012) Priv Observ Mag 2012(3).

BHM Custers, 'Data dilemmas in the information society', in BHM Custers, T Calders, BW Schermer, T Zarsky (ed.) Discrimination and privacy in the information society (2013, vol. nr. 3. Heidelberg: Springer)

BHM Custers, Click here to consent forever; Expiry dates for informed consent, (2016), Big Data Soc, 1–6.

BHM Custers & H Ursic, Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection (2016), Int Data Privacy Law 6(1): 4–15.

BHM Custers, S van der Hof, BW Schermer, S Appleby-Arnold and N Brockdorff, Informed consent in social media use. the gap between user expectations and EU personal data protection

law, in Script-ed: a journal of law and technology 10(4): 435–457, 2013
BHM Custers, S van der Hof B Schermer, Privacy expectations of social media users: the role of informed consent in privacy policies, (2014) Policy Internet 6(3): 268–95.
Exec. Office of The President of United States, Big data and differential pricing; 2015. Available from: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf. Accessed 12 June 2017, p. 17.
Gintare Surblyte, Data as digital resource, 2016. Max Planck Institute for Innovation & Competition Research Paper No. 16-12.
S Gnesi, I Matteucci, C Moiso, P Mori, M Petrocchi and M Vescovi, My data, your data, our data: managing privacy preferences in multiple subjects personal data, in B Preneel and D Ikonomou (eds.), Privacy technologies and policy, lecture notes in computer science, (2014) vol. 8450, pp. 154–71.
J Hancock John Hancock Introduces a Whole New Approach to Life Insurance in the U.S. that Rewards Customers for Healthy Living; 2015. Available from: http://www.johnhancock.com/about/news_details.php?fn=apr0815-text&yr=2015. Accessed 12 June 2017.
N Jentzsch, State-of-the-art of the economics of cyber-security and privacy, IPACSO – Innovation Framework for ICT Security Deliverable, No. 4.1, 2016.
N Jentzsch, A Harasser, S Preibusch, Monetising privacy – an economic model of the pricing of personal information, ENISA Report, Greece; 2012. Available from: https://www.enisa.europa.eu/publications/monetising-privacy. Accessed 12 June 2017.
M Kosinskia, D Stillwella, & T Graepelb, Private traits and attributes are predictable from digital records of human behaviour, in Proceedings of the National Academy of Sciences of the United States of America, 110(15): 5802–5805, 2013
N Lomas, Handshake is a personal data marketplace where users get paid to sell their own data', Tech Crunch; 2013. Available from: https://techcrunch.com/2013/09/02/handshake/. Accessed 28 May 2017.
J MacDonald, How much are your personal details worth? Bankrate.com; 2006. Available from: http://www.bankrate.com/nsccan/news/pf/20060221b1.asp. Accessed 12 June 2017.
G Malgieri, 'Ownership" of customer (Big) data in the european union: quasi-property as comparative solution?', (2016) J Internet Law, 20, n.5.
More-with-mobile, Prices and value of consumer data; 2013. Available from: http://www.more-with-mobile.com/2013/06/prices-and-value-of-consumer-data.html. Accessed 12 June 2017.
RG Newell, JV Siikamäki, Nudging energy efficiency behaviour: the role of information labels, 2014. 1 J. Association Environmental & Resource Economists 555.
A Odlyzko, Privacy, economics, and price discrimination on the Internet, 2003. Proceedings of the 5th international conference on Electronic commerce (ACM) 355.
OECD, Exploring the economics of personal data: a survey of methodologies for measuring monetary value, OECD Digital Economy Papers, No. 220, (2013, OECD Publishing).
OECD, Data-driven Innovation for growth and well-being, interim synthesis report, 2014.
C O'Neil, Weapons of math destruction; how big data increases inequality and threatens democracy, (2016, New York: Crown).
B Petkova and P Hacker, Reining in the big promise of big data: transparency, inequality, and new regulatory frontiers, 2016. Lecturer and Other Affiliate Scholarship Series. Paper 13.
C Prins, The propertization of personal data and identities, EJCL; 2004. Available from: www.ejcl.org/83/art83-1.html [Accessed 12 June 2017]. N Purtova, The Illusion of Personal Data as No One's Property (2015), Law, Innovation and Technology, vol. 7, n. 1, 2015.
B Reddix-Smalls, Credit scoring and trade secrecy: an algorithmic quagmire or how the lack of transparency in complex financial models scuttled the finance market, 2011. 12 U.C. Davis Bus. L.J. 87.
J Rose, O Rehse, and B Röber, The value of our digital identity (2016, New York: The Boston Consulting Group).
LH Scholz, Algorithmic contracts, 2016. Stanford Technology Law Review, Forthcoming. Available from: https://ssrn.com/abstract=2747701. Accessed 12 June 2017
DJ Solove, and DK Citron, Risk and anxiety: a theory of data breach harms, 2017a. Forthcoming. 96 Texas Law Review.
DJ Solove & DK Citron, Risk and anxiety: a theory of data breach harms, 2017b. GW Law School Public Law and Legal Theory Paper No. 2017-2.
E Steel, C Locke, E Cadman and B Freese, How much is your personal data worth?, Financial Times; 2013. Available from: http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz2z2agBB6R. Accessed 12 June 2017.
E Steele, Financial worth of data comes in at under a penny a piece, Financial Times, June 12, 2013.
S Wachter, B Mittelstadt, and L Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation. Int Data Privacy Law 2016, Forthcoming.
World Economic Forum, Rethinking personal data: strengthening trust; 2012. Available from: https://www.weforum.org/reports/rethinking-personal-data-strengthening-trust. Accessed 9 June 2017, p. 9.