Never Mind the Data: The Legal Quest over Control of Information & the Networked Self

Argyro P Karanasiou
Senior Lecturer in IT & Media Law
Centre for Intellectual Property Policy & Management
(CIPPM) – Bournemouth University
Bournemouth, UK
akaranasiou@bournemouth.ac.uk

Emile Douilhet
Doctoral Researcher - Media & Communications School
Centre for Intellectual Property, Policy & Management
(CIPPM) – Bournemouth University
Bournemouth, UK
edouilhet@bournemouth.ac.uk

***Abstract*— The paper discusses the theory of "propertization of data", namely the proposition that data can be owned and constitute one's property, in the light of big data and the quantified self (QS) movement. Can we really own our own data?**

Part 1 discusses the issue of commodification of personal data and part 2 dissects this further by examining how personal data is treated at each stage of the big data processing cycle. Parts 3 and 4 complete the argument put forth here, namely that raw data –once seen out of context and as a part of a dataset can indeed be considered as property, able to be owned and traded.

Keywords— big data; wearable tech; copyright; databases

I. THE COMMODIFICATION OF PERSONAL DATA & THE CONUNDRUM OF BIG DATA

Hardly a new area, Big Data has only recently been of particular interest for the legal scholars. In the aftermath of the Snowden revelations , the great power big data holds in determining the relations between public and private entities, posed some rather intricate legal questions, especially regarding the issues surrounding privacy of the online users [1] and the overall ethical challenges involved [2]. Many organizations now control vast amounts of raw data, and those industry players with the resources to mine that data to create new information have a significant advantage in the big data market. The use of predictive analytics in processing information tracked across different platforms to identify trends in the behavior of individuals further adds value to big data [3] and makes it an important asset for any commercial entity. This rapid commodification of personal data has given rise to a new approach with regard to its legal protection in the era of big data: a shift from the traditional privacy protection regime to a wider protection under property law is considered by scholars as an appropriate legal response to the phenomenon of monetization of personal data, once seen through the lens of Big Data [4].

This paper seeks to identify the legal grounds for the ownership of big data: who legally owns the petabytes and exabytes of information created, processed and stored daily? The users, the data analysts, the data brokers and all various info-mediaries could gain access and potentially claim ownership of this vast amount of information. At the same time, the advent of cloud computing has perplexed the matter of data ownership further: can data still be retained, once entrusted in the nebulous hands of a data-centre in the cloud?

The paper examines the various stages the Big Data processing cycle, with a view to outline how data can change hands, alter privacy expectations and even transform the data holder's legal entitlements, from privacy to property based claims. In doing so, it is attempted to provide a succinct overview of the legal ownership of big data by examining the key players in control of the information at each stage of the processing of big data and how is further complicated once cloud computing and data storage is added to the equation.

In this vein, an interesting paradox is revealed: whereas individual data may be hard to qualify for one's property, meriting extra protection, which stretches beyond the tight framework of data protection, datasets appear to be already under the direct control and ownership of data controllers, the latter being the primary beneficiaries of the value extracted from big data. The paper dissects this paradox by exploring additional normative (Quantified Self Movement, herein referred to as QS movement) and technological (Privacy by Design, herein referred to as PbD) measures put forth to aid user empowerment through ownership/control, complementing thereby the existing legislative framework, which mostly discusses data protection. This synergy of a user-centric legislative, normative and technological data protection measures is however currently fragmented and highly overlooked. It is ultimately contended that a robust data protection framework would presuppose that the uses acquires an active role inasmuch his personal data is concerned and should therefore address directly matters pertaining to data ownership.

II. THE CYCLE OF BIG DATA PROCESSING AND ITS LEGAL IMPLICATIONS: FROM PRIVACY TOWARDS PROPERTY.

It should be made clear from the onset that one of the major challenges for legal scholars discussing big data is the fact that the term itself is rather ambiguous and multiply defined [5], as it has been addressed in numerous fields and disciplines in the past few years. The Gartner report is at most cases a good point of reference: although it does not specifically use the term "big data", it describes the phenomenon of exponential increase of data (Volume) at an impressive size, rate (Velocity) and format range (Variety) [6]. For the purposes of this paper, we rely on this definition, as expanded by IBM, namely encompassing also issues pertaining to trust and security (Veracity) [7].

There are four main stages in the processing cycle of big data from its raw form to its use in predictive analytics: (i) collection (ii) processing (iii) mining, and (iv) usage. In the collection stage, raw data is collected through a number of means – either in a direct and voluntary manner by individuals themselves, or indirectly, inferred from the analysis of other data [8]. In the processing stage, data is aggregated in databases and is formatted to be ready for analysis, either by a corporation or by a third party (a "data processor"). It should be noted that at this point the information is transformed from its original crude form at the collection stage and becomes part of one or more large datasets, put together by one or more separate corporations. Then, in the data mining stage, all gathered and processed data is analyzed to create useful information. This new information created is essentially independent of the individual bits of information provided at the collection stage. Although it is the direct outcome of the analysis of segments of data from individual users, at this stage it also becomes the product of an analysis performed by entities completely separate from the data subjects, i.e. the users. Finally, in the usage stage, value is extracted from the information, through predicting analytics, data profiling, and any other number of methods able to exploit information for profit making. Having undergone through all these stages of data processing, data appears to be evolving from user-generated data, to mere data and to information (especially as part of a larger dataset); the latter might entitle data controllers to "own" the final output, as it will be seen in the remainder of the paper.

Before however one is able to determine whether there are any legal grounds for data ownership in any of these stages, a preliminary question must be answered first: do property rights apply to data? The idea of propertization of data, namely the protection of data under property or copyright law has been discussed extensively since the 1970s [9]. A major difficulty in addressing data as property is its intangible nature added to the fact that it can be replicated many times without concrete evidence that its value is lost. On the other hand, copyright law reviewed in general within a digital environment increasingly shaped by big data, is greatly challenged: works are used 'in bulk' for purposes other than making their content available to the public, such as text mining and content mining [10]. Personal data in that sense –although treated as a tradable commodity online- has not yet received explicit protection under copyright law regime, falling mostly within the protective scope of privacy law. Moreover, the European approach to privacy maintains a narrow conceptual approach, regarding this as a human right, which cannot be traded away [11].

As such, there is no explicit legal right of ownership for individual pieces of information. Were we to apply the legal concept of property to big data in any of the four stages mentioned above, we would need to carefully consider the main legal features of the concept of property in general: 'usus' (the right to use), 'abusus' (to right to encumber or transfer) and 'fructus' (the right to enjoy the right) [12]. In the absence of a formal right to ownership of big data, parties enjoying those rights should demonstrate these elements of ownership. Given the large amounts invested by the big data controllers, it would appear that the data collected and aggregated by corporations is under their ownership – they hold it in their databases, they process and aggregate it (usus), and they extract value from its analysis (fructus) and from selling it to other parties (abusus).

Nevertheless, data has a unique feature that complicates matters: the information is related to a person, gaining thereby an added aspect of privacy. Under the right to privacy, individuals enjoy a certain level of protection of their personal data, namely data able to identify them or to reveal private information about them without their consent. In this respect, the individual's right to data protection overrides the property right and economic interests of the data processors (Google Spain and Google Inc v Agencia Espanole de Proteccion de Datos of Mario Costeja, C 131-12, hereafter referred to as the "Google Spain" case).

One of the most robust legislative frameworks dealing with data protection is the EU Data Protection Directive 95/46 [13]. This provides us with a coherent legal regime, unlike the US data privacy law, which is at large scattered [14]. For this reason, the focus here is mostly on the EU data protection laws. The main three distinctions used in the EU Data Protection Directive are "data subject", "controller", and "data processor". A data subject is an "identified or identifiable natural person [...] an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.", while a "controller" means "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." Finally, a processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". It should be noted that the Directive uses words like "controller" and "processor" and avoids the appellation of "owner". Yet, although in none of the above definitions is the term ownership explicitly expressed, many provisions seem to suggest a property-based approach to data.

The Data Protection Directive establishes a number of rights for individuals relating to their data – such as the fact that collecting an individual's data requires their prior unambiguous consent (Article 7), that individuals should have access to their data (Article 12), or that they should be able to

object to the processing of their data if they have compelling legitimate grounds to do so (Article 14). The Directive also notably includes restrictions on what the data's controller can do with the data, including restrictions on the transfer of that data (Article 25). Drafted in 1995, the Data Protection Directive is currently undergoing reform after the finalization of the General Data Protection Regulation (GDPR) on the 6th of January 2016. The GDPR increases the rights that individuals hold over their data, as well as the restrictions of data controllers [15]. In particular, the restriction of what constitutes "consent" to the very high standard of "explicit consent" reinforces the idea that individuals have a property based right: the fact that ultimate control lies with the individual's consent is a clear indication of the data subject considered as data "owner". At the same time though, data can be processed without consent for a "legitimate interest pursued by a controller" (Article 6(1) (f) GDPR). Even though this provision is itself mitigated by the fact that "it shall not override the fundamental rights and interests of the data subject", the fact that the individual does not necessarily have a final say in what happens to their data tempers their power over the data.

That said, still the control that data controllers appear to have over personal data can be considered more of a substantiation of a claim to a limited form of "usus" - an ability to use data under certain circumstances, rather than a legal entitlement to data ownership. The right to data erasure/de-listing from the data subject on the other hand, again does not presuppose any level of ownership but appears to be a mere claim for "abusus" – the ability to ask for the data to be removed/ de-listed. The rights retained by data subjects as enshrined in the DPD and the GDPR seem to share this view as they point towards controllers only possessing limited "usus" and "fructus", with ultimately data subjects are able to lodge complaints for the "abusus" of their data.

III. Data Rights VS Database Rights: How Is Data Ownership Delineated, Once Decontextualized.

The data protection provisions in the Data Protection Directive and the upcoming General Data Protection Regulation have clear indications that individuals are granted certain rights over their data that extend beyond the traditional framework of privacy. Thus, as it was earlier demonstrated, data controllers demonstrate various elements of data ownership while processing big data; at the same time, under the right to be forgotten, it seems that at every stage, the data subject retains control over data being able to request erasure. This poses a legal conundrum: Can one be considered to own something in its entirety if at the same time someone else is further granted a right to command them to delist indexed data?

Although puzzling, it seems that the issues becomes less complicated if one takes into account that a distinction needs to be drawn between segments of personal data and databases built on such data. So far, the paper has explored the former; turning to explore now the latter, it appears that indeed there are strong indications in European law for specific provisions for a right to data ownership: the "database right".

The 1996 Database Right Directive 96/9 created a "sui generis" intellectual property right on data, the "database right" [16], namely "the right to prevent extraction and/or reutilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database." Unlike other intellectual property rights, a database right does not require an original or technical achievement as a prerequisite for affording copyright protection. In fact, a person can have a database right provided that he a substantial investment is made in obtaining, verifying, or presenting data in the database [17].

In this sense, database rights are automatically granted, and do not require to be registered or applied for. As such, the data constituting a database is not itself owned per se – it is rather the database in its entirety, having required time and effort to establish, that is protected. As a result, database rights enshrine in law the current practice of data controllers, granting them thus significant rights over the data they accumulate. Even though personal data is still protected under data protection regulation for the individual, the aggregation, processing and analysis of large amounts of data from a database, appear to have a separate existence separate. Outside the protective remit of privacy, databases are not protected as parts of the individual's identity and can thus be legally owned when one has a "substantial involvement" in it. As a rule of thumb, EU Courts generally accept that database rights can be legally owned, unlike their components, namely the segments of personal data compiled for a database. The first main guidance for the database right came in 2004 - 8 years after the adoption of the Directive - from four judgments of the European Court of Justice [18]: British Horseracing Board Ltd v William Hill Organization Ltd C-203/02 Judgment of the Court (Grand Chamber 2004); Fixtures Marketing Ltd v Organismos Prognostikon Agonon Podosfairou (OPAP) C-444/02 Judgment of the Court (Grand Chamber 2004); Fixtures Marketing Ltd v Svenska Spel AB C-338/02 Judgment of the Court (Grand Chamber 2004); Fixtures Marketing Ltd v OY Veikkaus Ab C-46/02 Judgment of the Court (Grand Chamber 2004). Most importantly, the database right in all these cases emphasize on the importance of organization and assemblage of data, not on the original creation of the data in a database. Investment in the creation of data does not trigger a database right, assemblage and presentation do.

It could be argued that a form of database right also exists in the US [19]: In a landmark US Supreme Court case, Feist (Feist Publications, Inc. v. Rural Telephone Service Co., Inc., 499 U.S. 340, 1991) copyright protection was extended to databases if there is originality in the "selection, coordination, or arrangement of contents for a database". Several cases since have built on this decision, and some state laws also provide from some protection for databases. The protection is however narrow ‡ [20] because of the originality requirement, in contrast to the wider EU provision, which puts the focus on the investment in the database and the arrangement of data.

IV. Out of sight, out of mind, "unless otherwise stated"? The nebulous case of data-custodians in the cloud.

In the previous section, the paper examined the concept of informational privacy in ubiquitous computing environments and delineated the regulatory scope for interconnected data flows, which involve critical amounts of user-generated content. As personal data is being processed and turns into information, so does its legal status transform from a key component of one's privacy to a part of someone else's (intellectual) property.

The relation between privacy and property is not a new one, nor is this the focus for this paper, as it has been frequently discussed in literature [21]. It is however extremely interesting to note that most scholars that approach privacy from this standpoint, refer to this as "control over informational autonomy" [22], inasmuch as the user decides to what extent his data is shared with others [23]. It has however thus far been shown, that once the link between the user and his data is broken at various stages of the big data cycle, not only is the data beyond his control but it might eventually be part of a dataset, owned by the private entity that curated it. The advent of cloud computing has augmented this further: the user has little knowledge of who his data is being stored, let alone where his data is being stored. Cloud computing provides an "underlying engine (for big data), through the use of (…) a class of distributed data processing platforms [24]. Although extremely effective in performing large scale computing for vast amounts of data, at the same time cloud computing poses many threats to the user's ability to fully be in control (usus, fructus and abusus) of one's data. To name a few examples:

i. Usus: Even though the user might still be regarded the legal owner of the data entrusted to a "data custodian", i.e. a cloud based data centre, the cloud provider may still be held liable and asked to comply with law enforcement authorities for providing them access to the user's data assets [25].

ii. Fructus: Many cloud services (e.g. LinkedIn) do not allow the user to fully retrieve information already provided, or even other services to access this data, even when authorised by the user [26].

iii. Absusus: A very good example in this respect, comes from a key aspect in big data security: 'data integrity'. In effect, this means that data normally has to be modified by authorizes parties or the user himself to prevent misuse. The fact though that most times, the user is not aware as to where the data is being stored, makes it very hard to maintain his data integrity [27].

The reason for this is mainly because cloud computing operates under the understanding that data transactions can be governed by contractual agreements between the user and the "data custodian". In contrast to data protection and a rights-based approach, in these instances data is merely a tradable commodity ruled by a pre-determined (and rarely negotiated) contract. Most users relinquish custody of their data, while having limited bargaining powers. At the same time, certain key issues (e.g. whether data is fully destroyed or returned to the users at the end of the contract) are not usually addressed [28].

Concerns over the limited privacy protection the user enjoys in the cloud have been voiced from both sides of the Atlantic: The Council of Europe Professional Informatics Society (CEPIS) [29] and the FTC in its report on "Protecting Consumer Privacy in the Era of Rapid Change" [30] list a few recommendation, however the matter of data ownership in the cloud is far from being resolved.

These concerns reveal also that personal data, seen from a legal perspective, once out of context, no longer qualifies for privacy protection and can only be regulated through a contractual agreement as a mere tradable commodity. The role that context plays in defining privacy has been highlighted by numerous legal scholars (Warren and Brandeis 1890; Scanlon 1975; Nissenbaum 2004). Assuming however, that a context reflects the norms and expectations of protecting data of certain value, it could be argued that informational privacy in the era of big data directly correlates to its valorisation, rather than to its context. What is argued here is that privacy may still apply to decontextualized data, if it can be owned. Personal data considered as an individual's property could bear legal entitlements to a digital personhood for the user, even when it exits one's personal sphere. The dichotomy of public/private sphere –frequently used as a legal criterion- is no longer a sufficient tool towards a legal assessment of informational privacy in a hyper-connected environment. The "domestic sphere" can no longer act as a bulwark to market forces in the era of cloud computing [31]; as a result a tight data protection framework can only afford limited protection. What is suggested instead is a normative approach of the right to privacy as an expression of one's property (informational integrity) beyond any "external efforts to render it orderly and predictable" [32]. This is a necessity, especially given the lack of a robust and harmonised legal framework with regard to cloud based data centres [33].

V. Challenges Posed By Wearable Tech: Collect Your Own Data and Own it Too?

So far it has been contended that although there is no explicit property right in data per se, there seems to be leeway for a property right to apply as far as databases are concerned. In addition, the advent of cloud computing has further distanced data from its original context, and the frequently evoked principle of public/private spheres (determining privacy expectations), appears to be of limited help to restore the link between the user and one's own generated data. At the same time, the nascent social phenomenon of QS is on the rise; namely users who use ubiquitous computing to collect and monitor (mostly health related) data. Are the current legislative and normative measures, as briefly discussed above, sufficient to address the paradox of a user willingly performing a "self-surveillance" exercise [34] to gather one's own data?

The rise of wearable tech, namely devices with sensors measuring the user's daily activities and habits has now posed a new legal challenge: how is legal ownership determined when a dataset is created and curated by the user himself? The growing tendency to self –track and quantify has taken off since its start in 2008 when two former Wired magazine

editors, Gary Wolf and Kevin Kelly, cofounded the "Quantified Self" digital tracking group. The term is now used to describe the mainstream phenomenon of adults collecting data as means of recording and analyzing their lifestyle [35]. It is estimated that 60% of US adults are currently tracking their weight, diet and exercise routine [36], actively collecting and analyzing their data in the context of their individual experiences [37]. Although there is still a corporation acting as a data controller by providing tools for data analysis and storage on their servers, the user can also extract value from this data; this blurs the boundaries of the legal ownership of these commonly created datasets. This issue poses further legal questions, once online health repositories are considered: Microsoft Health Vault and Dossia are two examples of companies offering patients the chance to voluntarily store, collect and share health information with health providers and family members or other users [38].

Tim Berners Lee at the 2014 IP Expo Europe stressed the importance of data subjects owning their data instead of the corporations for the purposes of creating "rich" data, namely big data that if merged can be profitable for both the user and the corporations. Although the law has not yet offered a concrete answer to the issue of ownership of such "quantified self" datasets [39] co-created by the users and the corporations, there is a growing tendency to allow the user for more control and ownership rights over his data with techno-legal solutions and alternative market models [40].

Personal Data Vaults (PDS) are currently one of the main technical solutions put forth in order to allow the user to gain control of his data back from the various corporations acting as info-mediaries in the big data market. The idea is to a privacy enhanced architecture enabling the user to access, control and trace their data once shared online [41]. In this vein, there are many suggestions employing technical means for the user to reclaim control over his data: Once such example is the MIT Open PDS app, which allows the user to see third-party requests for his data and make informed decisions [42]. An alternative means of user-controlled data comes from Cozy cloud, a French company that provides users with open sourced private clouds to store their personal data. Other examples include a rising number of start-ups, such as "Personal", "Reputation.com" and "Datacoup", whose aim is to help the user monetize and control own data. That said the law is still admittedly lagging behind in terms of providing user with more control over his data [43].

Many countries have embraced user-controlled data as a promising economy boosting strategy: The Midata project, announced in 2011 in the UK, is a multi-stakeholder approach to boost consumer empowerment by giving "consumers increasing access to their personal data in a portable, electronic format" enabling them to "use this data to gain insights into their own behavior, make more informed choices about products and services, and manage their lives more efficiently" [44]. Mydex and HatDex have further adopted a community platform model to build PDS (Personal Data Stores) that enable users to manage, share and deploy their data [45]. Similarly in the US, the Federal trade Commission (FTC) in its report entitled "Data Brokers: A Call for Transparency and Accountability" issued in May 2014, calls for tighter regulation of the data brokers, namely large companies trading the user's data without the user's knowledge or consent.

At present, data controllers have the most control over data under the database right protection and are thus the primary beneficiaries of the value extracted from big data ('fructus'); at the same time, there seems to be a slight shift towards empowering the user to control and perhaps "own" his data, although legally this is yet to be fully established. It is suggested that a mixed approach using the normative, technological and legal means briefly discussed in this paper, could restore the link between the user and his data, currently a "foggy" matter in the cloud.

ACKNOWLEDGMENT

‡ The authors wish to thank Peter Hirtle, Senior Policy Advisor (Cornell University Library) for bringing this point (p.3 ft. 18) to our attention. We also wish to thank the anonymous reviewers for their feedback, which has been extremely helpful towards refining certain parts of the paper. Any errors or omissions remain the sole responsibility of the authors.

REFERENCES

[1] Mayer-Schoenberger V & K Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (J Murray, 2013)

[2] Schroeder, R., 'Big Data: Towards a More Scientific Social Science and Humanities', in: M Graham and W H Dutton (eds) Society and the Internet: How Networks of Information are Changing our Lives (Oxford: Oxford University Press 2014)

[3] Fotopoulou A, 'Tracking Biodata: Sharing and Ownership' (2014) Report on Research Placement funded by the RCUK Digital Economy NEMODE Network

[4] Victor, J. M., 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 Yale Law Journal 513

[5] Ward, J. S., & Barker, A., 'Undefined by Data: a Survey of Big Data Definitions' (2013). *arXiv preprint arXiv:1309.5821*.

[6] Douglas, L. '3d Data Management: Controlling Data Volume, Velocity and Variety (Gartner 2001)

[7] IBM, What is Big Data? - Bringing Big Data to the Enterprise, available online at http://www-01.ibm.com/software/data/bigdata/, accessed 07/02/2016.

[8] Al-Kouri A, 'Data Ownership, Who Owns my Data?' (2012) International Journal of Management & Information, Volume 2, No 1

[9] Fromholz, J. 'The European Union Data Privacy Directive' (2000) Berk. Tech. LJ 15 461.

[10] Borghi M, Karapapa S, Copyright & Mass Digitisation (Oxford: Oxford University Press, 2013)

[11] Prins, J. E., 'The propertization of personal data and identities' (2004) Electronic Journal of Comparative Law 8.3.

[12] Segal, I, & Whinston, M, Property Rights: Handbook of Organizational Economics (2012) 100-158.

[13] Levin A & Nicholson M J, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005) U of Ottawa Law & Technology Journal, Volume 2 (2), 362.

[14] Gaff, B. M., Smedinghoff, T. J., & Sor, S. (2012) 'Privacy and Data Security' Computer (3), 810.

[15] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, 9 April 2014.

[16] Rendie, A., Aggregation: Demystifying Database Rights (Taylor Wessing, 2011)

[17] Reichman, J & Samuelson, P, 'Intellectual Property Rights in Data' (1997) Vand. L. Rev. 50

[18] Aplin, T, 'The ECJ Elucidates the Database Right' (2005) Intellectual Property Quarterly.

[19] Wu, X 'EC Data Base Directive' (2002) Berkeley Tech. LJ 17 571.

[20] Gervais, D. J. 'The Protection of Databases' (2007) Chi.-Kent L. Rev. 82 1109.

[21] Kahn, J. 'Privacy as a Legal Principle of Identity Maintenance' (2002) Setton Hall L. Rev. 33 371.

[22] Tribe, L. American Constitutional Law (Foundation Press 1988) 1302

[23] Gavison, R. 'Privacy and the Limits of Law' (1980), Yale L. J. 89 421. 423.

[24] Hashem, I. et al, 'The Rise of Big Data on Cloud Computing: Review and Open Research Issues' (2015) Information Systems 47 98,110.

[25] Winkler, V. Securing the Cloud (Syngress 2011).

[26] Gray, D. 'Data Ownership in the Cloud' (2014), available online http://dataconomy.com/data-ownershio-inpthepcloud /(accessed 2/2/2016)

[27] Hashem, I. et al, (n 24) at 102.

[28] Schissel, N 'Cloud Computing, Sata Secutiry and Privacy Issues' (2014) http://technologylawadvisor.com/cloud-computing-data-security-and-privacy-issues/ (accessed 2/2/2016).

[29] CEPIS, 'Cloud Computing Security and Privacy Issues', available online https://ec.europa.eu/digital-agenda/events/cf/cloud-computing-software-engineering/document.cfm?doc_id=30676

[30] Federal Trade Commission Report, 'Protecting Consumer Privacy in an Era of Rapid Change', available online https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[31] Take for example the use of encryption, which does not necessarily constitute a reasonable expectation of privacy. Cf Kerr, O. 'The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?'(2001) 33 Conn L Rev 503

[32] Cohen, J E, 'The Inverse Relationship between Secrecy and Privacy' (2010), Social Research 77 883,896

[33] A good example of how this normative approach can be applied on the cloud can be found in Grodzinsky,F & Tavani, H. 'Privacy in the Cloud: Applying Nissenbuam's Theory of Contextual Integrity' (2011) ACM SIGCAS Computers and Society 41.1 38

[34] Karanasiou, A & Kang, Sh, 'My Quantified Self, My FitBit and I: The Polymorphic Concept of Health Data and the Sharer's Dilemma' (2016) Digital Culture and Society: Quantified Self, Statistic Bobies (special issue, forthcoming.)

[35] Haddadi H & Brown I, 'Quantified self and the privacy challenge' (2014) Technology Law Futures.

[36] Swan M, The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery (2013) Big Data, Vol 1.

[37] Nafus D & Sherman J, 'This One Does Not Go Up to 11: The Quantified Self Movement as an Alternative Big Data Practice' (2014) International Journal of Communication 8, 1784–1794.

[38] Steinbrook R, 'Personally Controlled Online Health Data – The Next Big Thing In Medical Care?' (2008) N Engl. J Med 358 16

[39] Purtova N., Property Rights in Personal Data: A European Perspective (Kluwer, 2011)

[40] Novotny A & Spiekermann S, 'Personal Information Markets AND Privacy: A New Model to Solve the Controversy' (2013) 11th International Conference on Wirtschaftsinformatik, Leipzig, Germany.

[41] Mun M, S Hao, N Mishra, K Shilton, J Burke, D Estrin, M Hansen, R Govindan, 'Personal Data Vaults: A Locus of Control for Personal Data Streams' (2010) ACM CoNext.

[42] de Monjoye, Y-A, Shmueli E, Wang SS, Pentland AS, 'Open PDS: Protecting the Privacy of Metadata through SafeAnswers' (2014) PLoS One 10, 1371.

[43] Crawford K, Miltner K, Gray M, 'Critiquing Big Data: Politics, Ethics, Epistemology (2014) International Journal of Communication 8, 1663; Boyd D, Crawford K 'Critical Questions for Big Data: Provocations for a Cultural, Technological and Scholarly Phenomenon' (2012) Information, Communication & Society 15 (5), 662.

[44] Department for Business & Innovation Skills, The Midata Vision of Consumer Empowerment (2011), available online at https://www.gov.uk/government/news/the-midata-visionofconsumer-empowerment (accessed 14/03/2015).

[45] https://mydex.org/understand-pds/, accessed 07/02/2016. Our thanks to the anonymours reviewers, who brought this to our attention.