IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTICLE

Slaves to Big Data. Or Are We?

Mireille Hildebrandt
Chair of Smart Environments, Data Protection and the Rule of Law
Institute for Computing and Information Sciences (iCIS)
Radboud University Nijmegen

Received: October, 2013
Accepted: October, 2013
Published: October, 2013

Abstract
In this contribution, the notion of Big Data is discussed in relation to the monetisation of personal data. The claim of some proponents, as well as adversaries, that Big Data implies that 'n = all', meaning that we no longer need to rely on samples because we have all the data, is scrutinised and found to be both overly optimistic and unnecessarily pessimistic. A set of epistemological and ethical issues is presented, focusing on the implications of Big Data for our perception, cognition, fairness, privacy and due process. The article then looks into the idea of user-centric personal data management to investigate to what extent it provides solutions for some of the problems triggered by the Big Data conundrum. Special attention is paid to the core principle of data protection legislation, namely purpose binding. Finally, this contribution seeks to inquire into the influence of Big Data politics on self, mind and society, and asks how we can prevent ourselves from becoming slaves to Big Data.

Keywords
Big Data, artificial intelligence, monetisation of personal data, user-centric personal data management, double contingency

Topic
Big Data

Esclavos de los macrodatos. ¿O no?

Resumen
En este trabajo se debate la noción de macrodatos con relación a la monetización de los datos personales. Se revisa lo que afirman algunos de sus defensores y adversarios, según los cuales los macrodatos implican que «n = todos», en el sentido de que ya no es necesario utilizar muestras, puesto que disponemos de todos los datos, y se llega a la conclusión de que tal argumento es al mismo tiempo demasiado optimista

e innecesariamente pesimista. Se presenta una serie de aspectos epistemológicos y éticos relacionados con las repercusiones de los macrodatos en nuestra percepción, cognición, imparcialidad y privacidad así como en los debidos procesos legales. A continuación, el artículo examina la idea de la gestión de datos personales centrada en el usuario, para averiguar hasta qué punto este tipo de gestión aporta soluciones a algunos de los problemas planteados por el enigma de los macrodatos. Se presta una especial atención al principio básico de la legislación sobre protección de datos, concretamente el principio de finalidad vinculante. Para terminar, este trabajo pretende indagar en la influencia que tiene la política de los macrodatos en la persona, la mente y la sociedad, y preguntarnos cómo podemos evitar el convertirnos en esclavos de los macrodatos.

Palabras clave
macrodatos, inteligencia artificial, monetización de los datos personales, gestión de datos personales centrada en el usuario, doble contingencia

Tema
macrodatos

Introduction

The problem with Big Data is that n = all.[1] Or rather, the problem is the claim by some of its advocates (and adversaries) that n = all. 'N = all' nicely summarises what Big Data is about, how it is defined and which are its pitfalls. *If it were true*, Big Data could rupture any membrane that shields our inner lives, disrupting the most sacred place of both privacy and autonomy, because it would allow its masters to know us better – and to know anything better – than we do ourselves. *If it were untrue*, Big Data could still uproot our sense of self and our interface with the world, because to the extent that we could not contest its outcomes, we would have trouble resisting the seemingly clean, objective knowledge it produces and we would not have the tools to determine how we are being profiled. *If untrue*, Big Data will generate incorrect discrimination, but even *if true* Big Data can generate unfair or unjustifiable discrimination.

The problem is, of course, that speaking in terms of true or untrue in relation to Big Data does not make sense, because Big Data is about data modelling. Whether top-down or bottom-up, automated or even autonomic, it is better to ask whether the modeling works, what its effects are and how these effects are distributed. Finally, and most importantly, the question is what kind of humans will we become when interacting with the models that Big Data generates to figure us out with. I have already succumbed to speaking of Big Data as 'something' that figures us out. As if Big Data has a mind of its own. It would be so simple to deny this and attribute its predictions to the designers of Big Data technologies or to their users, the advertising networks, data brokers, justice authorities, scientists, smart grid operators and any other service providers that base their decisions to grant a credit, a job or insurance on Big Data. Or to the service providers that outsource their decisions to the high-speed, real-time autonomic computing systems that increasingly determine our external environment. Take for example the preparations for the Smart Grid that will combine real-time processing of our energy usage data with flexible pricing to enable us to upload energy to the grid and sell it to our nearest neighbours.[2] IBM has coined the term *autonomic computing*, suggesting that autonomous computing systems will adapt our external environment just as the autonomic nervous system 'runs' our internal environment: in ways to which we have no conscious access, and over which we have no direct control.[3] To the extent that Big Data is smart enough to operate autonomically, however, it must outsmart

1. In quantitative empirical research, 'n' stands for the sample, whereas 'all' would refer to the entire population. If 'n' were 'all', we would no longer be referring to a sample because we would be researching all the instances of whatever it is we want to investigate.
2. Hildebrandt (2013a).
3. Kephart *et al.* (2003, pp. 41–50).

both its designers and its users. Big Data is smart because it generates solutions we could not have developed, since as humans we do not have enough computing power. So, the use of Big Data generates unpredictability similar to that of an animal: however well trained, we cannot entirely control its behaviour. Worse still, it may generate the volatility of volcano eruptions – of 'acts of god' as we once called them. It might be that, to the extent that we worship Big Data, believe in it and make ourselves dependent upon its oracles, it turns into a new pantheon, filled with novel gods – gods of our own making, but not necessarily under our control. This indicates that it may indeed be wise to speak of Big Data having a mind of its own, without suggesting that its mind is like our mind, and without forgetting that its mind is developed initially by businesses, scientists and government agencies to make a profit, to construct new knowledge and to improve the efficiency and effectiveness of public administration.

In this contribution, I want to raise the question of the double contingency – the mutual interdependence – between Big Data, individual minds and human society. To do so, I will begin by (I) investigating how Big Data has been defined, including the provocations this has generated from those at home in the field of data science. I will then look into some of the solutions being offered (II), for instance by the World Economic Forum, to re-establish some form of balance between individual persons and the corporations who practically own the data relating to them. I will then also discuss one of the core principles of constitutional government: purpose binding (III) – firmly rooted in the principle of legality (not to be confused with legalism). In the realm of personal data processing, this principle relates not only to Big Data in the hold of data-driven governments, but also to the business models of private companies that monetise Big Data. To what extent is the sharing, selling and further processing of personal data beyond the context of its collection lawful and/or ethical? Is Big Data analytics compatible with prior purpose specification? Or is function creep the holy grail of Big Data, and is cross-contextual data mining what makes for the added value in science, business and administration? Must we rethink purpose specification as it is entirely at odds with the internal logic of Big Data? I will conclude (IV) by returning to the question of the mutual interdependence of Big Data, individual persons and human society.

1. Defining Big Data: 'N = All'

If you want to improve the performance of your website, you can do AB research.[4] This means you make a small change to the layout of your site A and direct half of your visitors to site A and the other half to site B, which is the same site but with minor changes. You then log everything the visitors do and calculate how the two versions of the site match for preferred behaviour (say, purchasing behaviour). Instead of taking a sample of your website visitors and calling them or sending them an email, you simply measure the behaviours of your visitors and act on the findings. You no longer depend on the subset that responds, and there is no bias from people who provide you with politically correct answers. You do not have to settle for what people say they did or will do – you can just calculate what they did, do and will probably do. We, those visitors, are your guinea pigs, though nobody asked for our consent to engage in this experiment, nobody paid for our contribution to improve the performance of the website and, in fact, we never even noticed we were doing so.

The Big Data Conundrum: implications of a game changer

In their breathtaking *Big Data. A Revolution That Will Transform How We Live, Work and Think*, Mayer-Schönberger and Cukier describe Big Data as referring to:

> things one can do on a large scale that cannot be done on a smaller scale.[5]

This is an important starting point, because obviously Big Data is not merely about a big bag of data. The complementary dimension, which is part and parcel of the notion of Big Data, is constituted by the techniques to mine relevant patterns from stored or even streaming data. These techniques have been named knowledge discovery in databases (KDD) and most of them are now associated with machine learning. KDD has been defined as:

> [T]he nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data.[6]

4. Kohavi *et al.* (2007); Chopra (2010). See also eg.: <http://elem.com/~btilly/effective-ab-testing/>.
5. Mayer-Schönberger *et al.* (2013, p. 6).
6. Fayyad *et al.* (1996, p. 41).

Machine learning has been defined as:

> A machine learns with respect to a particular task T, performance metric P, and type of experience E, if the system reliably performs its performance P at task T, following experience E.[7]

Both form the core of *Artificial Intelligence: A Modern Approach (AIMA)*,[8] not to be confused with Good Old Fashioned Artificial Intelligence (GOFAI). The latter was based on deductive models, rule-based or case-based, assuming that intelligence could be modelled and replicated based on a formal model of human intelligence. The modern approach, notably machine learning, is based on the notion of agency, defined as the capability to be interactive, autonomous and adaptive.[9] I know that many authors still have doubts about machines that learn, but I think it is more productive to admit that machines are indeed learning, at high speed, and in a manner both different and similar to how we learn. This does not imply that machines think like we do, or feel as we may. It does raise the question of whether our own learning processes are beginning to change as a consequence of having to interact with learning machines. What does autocomplete do to our way of writing? How does it impact our fluency in language? Which productive misunderstandings does autocomplete generate between communicating friends? Remember that Zizek wrote that communication is a successful misunderstanding,[10] meaning that we can never really look into each other's minds, we can never be sure whether we mean the same thing with the same words. He reminds us that this is not a problem to be solved, but a source of creativity. Is autocomplete, which nicely forebodes other types of smart environments, like ambient intelligence and the Internet of Things,[11] a source of creativity, or does it aim for perfection and will it in the end take over the production of meaning, though from the perspective of a machine? Will we internalise the drive for disambiguation that is inherent in machine language and will we come to believe that disambiguity equals perfect communication? In other words, the question is not whether machines can 'really' learn, but whether we will become more like machines because that will make it easier to anticipate how they anticipate us? And if so, is there something important in human learning, human thought and human feeling that we want to preserve?

Let us, however, first follow Mayer-Schönberger and Cukier in their quest to explain Big Data. Their analysis starts with the notion of 'n = all'. In traditional quantitative research, scientists that aim to uncover regularities in a population were forced to investigate a sample, relying on statistics to extrapolate from the sample to the population. Examining the whole population was simply impossible or too costly. A population can be a set of people, but also a set of animals, plants, stones, landscapes, cells, molecules or any other entity, event or process. So, the research starts with a hypothesis that is tested on the sample. The sample consists of 'n' instances of the relevant population, suggesting that, to the extent that the sample correctly represents the population, the findings on the sample will hold for the population. Such traditional research requires developing the hypothesis, composing a representative sample, conducting the research and calculating the conclusions, which take time, expertise in the relevant subject matter and – depending on the kind of testing to be done – may also require expensive instruments. Whatever the conclusions, they remain uncertain due to the fact that it is not possible to collect all the relevant instances of the population.

'N = all' means that the sample equals the population. It implies that the uncertainty generated by the jump from sample to population is absent in the case of Big Data. Or, more moderately formulated, it means that the exponential increase in 'n' substantially reduces this uncertainty. This is linked to the idea that the availability of nearly all instances of a given population compensates for potential inaccuracies. Mayer-Schönberger and Cukier indeed claim that lack of precision in some instances will be corrected by subsequent recordings of further data. The growth of knowledge that is made possible by having 'n = all' invites further 'datafication', promising endless opportunities to mine the data in search of new relevant patterns. This is the case because such patterns may enable new business models, or – in the case of public administration – new business cases for more efficient and effective governance.

7. Mitchell (2006).
8. Russell *et al.* (2010).
9. Floridi *et al.* (2004, pp. 349-379).
10. Zizek (1991, p. 30).
11. Van Den Berg (2010); Aarts *et al.* (2003).

We can say that 'datafication' is the process of translating the flux of life into discrete, machine-readable, measurable and manipulable bits and bytes.[12] Datafication reinforces the illusion of 'n = all', because it enables seemingly unlimited discretisation due to the reduction of costs of and the exponential increase in computing power.

The current explosion of data actually does two things. First, it turns data into noise: the sheer quantity of bits and bytes makes them unreadable to the human eye. Second, to turn this noise into information or even knowledge, computational techniques of information retrieval have been developed and applied. And as indicated earlier, this is not merely about queries that retrieve the original input, but increasingly about mining operations that retrieve patterns not previously uncovered – invisible patterns derived from statistical inferencing. Such inferences can be termed 'data derivatives' as Louise Amoore aptly suggests.[13] Data derivatives that provide for *present futures*, or in other words, anticipations of the *future present*. And, as Elena Esposito has argued,[14] these *present futures will shape the future present*. The better the predictions (the present futures), the more people may act on it and thus change the cause and the course of the future present.

In the meantime, as Mayer-Schönberger and Cukier note, the speed with which new data become available and the speed with which correlations within the data sets can be mined AND tested, seems to suck the life out of the quest for causality. This is rapidly becoming an old-school quest, a search for 'why' in an era that works better on 'how, when, where, depending on what', with no time to sort out the causes 'behind' the correlations. Because by the time you have started your investigation, the correlations may have been falsified, shown to be spurious or simply followed up with novel correlations that 'work' better. This point has been made many times, notably by Chris Anderson in his provocative article in *Wired Magazine* "The End of Theory".[15] Indeed, the shift from causation to correlation is based on a consequentialist understanding of meaning; to explain the meaning of a correlation one does not revert back to causation but one looks forward to what it might effect. From the perspective of philosophical pragmatism, this is fascinating: it reminds one of the so-called pragmatist maxim on the meaning of concepts. This maxim seems particularly 'apt' for the era of Big Data if we replace *conception* with *correlation* or *pattern*:

> Consider what effects, which might conceivably have practical bearings, we conceive the object of our conception to have. Then, our conception of those effects is the whole of our conception of the object.[16]

The next big thing that Mayer-Schönberger and Cukier discuss is the shift from expertise to data analysis. There seems to be no field in which data analysis is not emerging as a game changer, realigning work processes, methodologies, business models and business cases. The exposure of the secret surveillance practices of the NSA by a system administrator are a case in point[17]. To survive, both the industry and government must adapt their decision systems in line with data processing operations that progressively dictate what is possible, thus enabling as well as limiting how we perceive the world. This then raises the question of free will. Mayer-Schönberger *et al.* suggest that we are on the verge of data dictatorship, meaning that we become incapable of perceiving reality outside the mediation of Big Data techniques and technologies. The authors thus propose that data, data mining, machine-to-machine communication and computational decision systems may soon take over.

N is not All and All is not N

It seems that Mayer-Schönberger and Cukier start with somewhat unwarranted techno-optimism and finish with similarly unwarranted techno-pessimism. I will now briefly discuss the six provocations developed by Boyd and

12. Manipulation is used here in the neutral sense of altering, editing or moving text or data on a computer in a skilful manner. The ability to manipulate bits and bytes may result in the capability to manipulate a person in the pejorative sense of controlling or influencing a person or a situation cleverly, unfairly or unscrupulously.
13. Amoore (2011, pp. 24-43).
14. Elena Esposito (2011).
15. Anderson (2008). Still earlier philosopher of science Isabelle Stengers traced the way correlations operate in the era of data mining: actually producing meaning instead of uncovering previously existing causes or reasons, eg. Stengers (1997, pp. 62-63).
16. Peirce (1958).
17. Davidson (2013).

Crawford[18] against the Big Data conundrum. First of all, Boyd *et al.* agree that automated research changes our definition of knowledge. Big Data is not just another addition to knowledge generation or knowledge management. It is a game changer. It implies another understanding of what counts as knowledge and creates different underpinnings for human, machine-to-machine and hybrid decision systems. Contrary, however, to Mayer-Schönberger and Cukier, they do not believe in 'n = all'. Claims to objectivity and precision are misleading. I would suggest that this is related to the fact that quantification always implies a preceding qualification. To translate the flux of life into discrete, machine-readable bits and bytes, we must qualify what counts as the same type of data, what realities fit what objects and attributes in the data models used to map Big Data. This entails interpretation. As has been noted,[19] there is no such thing as 'raw data' – data are made, just like facts. As the French say: 'les faits sont faits'. In that sense, N is never All, because the flux of life can be translated into machine-readable data in a number of ways and whichever way is chosen has a major impact on the outcome of data mining operations.

In line with this, Boyd and Crawford claim that Bigger Data is not always Better Data nor necessarily Whole Data; sometimes Small Data is Best Data. Now, here we have a truly revolutionary statement, as far as the Big Data conundrum goes. I believe that for data scientists this is nothing new or surprising. Time, human expertise and computer power are scarce – contrary to what some Big Data believers like to announce. The translation of entities, events and processes into discrete data requires the interpretation of such entities, events and processes and requires reiterant anticipation of what a specific data model will effect, and how it will enable and restrict the outcome of data mining operations.

This relates to Boyd and Crawford distinction of *social networks* between humans of flesh and blood, on the one hand, and *behavioural networks* or social graphs observed by the software machines of service providers, on the other. Mistaking machine-readable behaviours for action seems part of the business case for predictive analytics. Though this may be a very productive 'mistake', it might in fact trigger a situation where behaviours draw the curtain on action: who cares whether you had reasons or intentions if your behaviours correlate with your genetic disposition, match your online social graphs or the combined data collected by government agencies in the course of your life? Boyd *et al.* thus set the stage for two ethical issues.

1. Does the fact that personal data are publicly available render their exploitation and monetisation ethical?

2. Should we accept the novel inequalities created by the knowledge asymmetries between data subjects and data controllers?

   We can add four epistemological issues that incorporate a number of less obvious but far more pervasive ethical issues:

3. Traditional natural and social sciences start from theoretical reflection that is tested by deriving a hypothesis that can be checked against a sample (this is called falsification and is supposed to create robust knowledge). What does it mean to skip the theory and to limit oneself to generating and testing hypotheses against 'a' population?

4. Data science provides for a number of alternative techniques to detect patterns in data sets, which will often have alternative outcomes. If public and private service providers mostly employ only a subset of such techniques, what does this mean for the robustness of such outcomes and for the extent to which they should inform the architecture of autonomic computing systems?

5. In the old days we said 'if men define a situation as real, it is real in its consequences' (Thomas Theorem).[20] Now we must admit 'if machines define a situation as real, it is real in its consequences'. What does this mean for the salience and the bias of the decision systems that depend on Big Data analytics?

6. If the intestines of these decision systems are opaque to those affected by their operations, and even to those who operate them, where does this leave democracy and the Rule of Law? Are due process and fair administration, informed consumer choice and the right not to be subject

18. Boyd *et al.* (2012).
19. Gitelman (2013).
20. Cf. Merton (1948, pp. 193-210).

to invisible decision-making on the verge of becoming illusive concepts?

2. Personal data management in the era of Big Data

Volunteered, Observed and Inferred data

Let us return to the AB experiment. The data are mined to improve the user experience, the website's performance, or the profitability of the business model, but they are not volunteered by the visitor. No forms are filled, no questions asked. The data here are observed data, and they usually consist of behavioural data. In its project on *Rethinking Personal Data*, the World Economic Forum (2013) recently launched a report entitled *Unlocking the Value of Personal Data: From Collection to Usage*.[21] One of the key aspects of their supposedly new approach includes 'new ways to engage the individual, help them understand and provide them with the tools to make real choices based on clear value exchange'. This is very interesting. For a long time, the value of personal data has been seen as related to an individual's personality. German legal doctrine, for instance, understands the fundamental rights to privacy and data protection as personality rights, meaning that they are related to the dignity and autonomy of a person and should be seen as constitutive for the self;[22] not as something to trade with. In the realm of consumer-business relations as well as iGovernment, the legal framework of EU data protection is focused on data minimisation. As consumers or as citizens, people should only provide the data that are necessary for a specific purpose and their usage is only lawful as long as this purpose (or a compatible purpose) holds. This also holds when the data are provided with consent.[23] However, once we begin to think in terms of 'a clear value exchange' and speak of personal data as 'a new asset class', the monetary value of personal data is indeed unlocked. In a previous report, the WEF actually highlights this point by stressing the hidden potential of personal data as 'untapped opportunities for socioeconomic growth',[24] urging a renewed discussion of the collection and usage of such data that takes into account the current monetisation of personal data. This renewed discussion starts from an alternative typology of data, clearly distinguishing between volunteered, observed and inferred data, rather than between personal and non-personal data. Traditional data protection legislation still seems focused on volunteered data, even in the case of third-party access to personal data or in the case of legal obligations to provide data. Volunteered data are defined as 'created and explicitly shared by individuals, eg. social network profiles'. I would add that all the forms you fill and credit card data you consciously provide are volunteered data. Note that the distinction between volunteered and observed data is not about whether a person has provided consent or even about whether they should be considered personal data. The processing of both types of data may involve or even require consent and they may both be qualified as either personal or non-personal data, e.g. depending on the use of anonymisation techniques. The business case for AB research, traffic management, NSA spying programs, law enforcement or fraud detection is seldom restricted to the processing of volunteered data. It is more often based on observed data, usually behavioural data, measured by the software machineries that mine, share and sell such observed data to attain the holy grail of Big Data, which is inferred data. So, we have volunteered, observed and inferred data and I dare say that these different types of personal or 'unpersonal' data require differential legal protection.[25] It is one thing to consent to the sharing of credit card data in order to buy something online, or to the sharing of a photograph posted on Facebook, and an altogether other thing to consent to machine-to-machine sharing of your online behaviours, or to the sharing of your public transport behaviours or your biometric behaviours. Moreover, the inferred data, e.g. profiles derived from data mining anonymised aggregated data, may have the biggest impact on a person. If three or four data points of a specific person match inferred data (a profile), which need not be personal data and thus fall outside the scope of data protection legislation, she may not get the job she

21. World Economic Forum (2013).
22. Rouvroy *et al.* (2009); G. Hornung *et al.* (2009, pp. 84-88).
23. De Hert *et al.* (2006).
24. World Economic Forum (2011).
25 Unpersonal data is neither personal nor non-personal in the sense that the distinction is not relevant. Anonymised and inferred data may be non-personal data as far as art. 2(x) Directive 95/46 EC is concerned, but when applied to an individual person its impact may be more substantial than the use of volunteered data.

wants, her insurance premium may go up, law enforcement may decide to start checking her email or she may not gain access to the education of her choosing.

Under the EU data protection framework, however, there is a right not to be subjected to such profiling to the extent that it is fully automated.[26] There are three major exceptions to that right: consent, contract and a legal obligation. If such an exception applies, there is a transparency right: we must be told that profiling has determined the decision and we must get information on how different factors were weighted. To become an effective right, those who employ the data analytics that significantly impact a person should provide transparency of the backend system (what the software is actually doing) in a clear and comprehensible manner. And, since end-users should not be entirely dependent on those who 'own' the data servers and machine learning technologies, they will require their own transparency tools, i.e. on the frontend of the system. Such transparency tools can be created as platforms run by consumers or trusted third parties that allow consumer data to be shared and mined to predict how the data will probably be monetised or how they might be used by law enforcement. Such platforms would employ inference engines to counter-profile the profilers or, in other words, to guess how we are being anticipated, to read how we are probably read and to pre-empt how our intentions might be pre-empted.[27]

User-centric Personal Data Management

This brings us to the solutions currently proposed. After the failure of large-scale employment of privacy-enhancing tools (PETs), followed by the notion of Privacy by Design (PbD), which has been taken up as a legal obligation in the proposed General Data Protection Regulation (GDPR) under the heading of Data Protection by Design (DPbD), the new kid on the block is called Personal Data Management (PDM).[28] This can best be understood as an attempt to build architectures and trust frameworks that should enable data minimisation and informed consent, with the hope of bringing end-users back into the equation of personal data ecosystems. I will not go into the technicalities but refer to the definition of Bus *et al.* (2013) of context-aware PDM as an ICT application that:

> enables an individual to control the access and use of her personal data in a way that gives her sufficient autonomy to determine, maintain and develop her identity as an individual, which includes presenting aspects (attributes) of her identity dependent on the context of the transactions (communication, data sharing, etc.), and enabling consideration of constraints relevant to personal preferences, cultural, social and legal norms.[29]

There are many vague terms here, but sometimes being more specific means reducing protection. Defining notions such as 'identity', 'sufficient', 'context', and 'consideration' will be necessary, but every further definition will also reduce the applicability of the concept – so we better leave such further definition to the operational level.[30] It is important to note that the term 'identity' is used here in two different ways. First as a reference to the self and second in the technical sense of the complete set of attributes that defines a person, or in the technical sense of one or more data points that uniquely identify a person. The idea behind PDM is that the use of technical identities has an impact on the development of identity in the sense of selfhood, meaning that the use of identities in the technical self should be restricted to protect identity construction in the sense of selfhood.[31] One way of achieving protection against 'unreasonable constraints on the construction of one's identity',[32] would be to employ PDM as an instrument for minimal disclosure, for instance by enabling authentication by means of attribute-based credentials instead of full identification. By only revealing the attribute that is necessary for the provision of a service (being under or over a certain age, male or female, having

26. Art. 15 of 12 D 95/46 EC and art. 20 of the proposed GDPR. On the differences see Hildebrandt (2012, pp. 41-56).
27. On the pre-emption of our intentions as a function of behavioural advertising, McStay (2011, p. 3).
28. Obviously many commercial entities and government agencies are literally managing other people's personal data. When I refer to PDM, I mean user-centred PDM, providing a measure of control to the person to whom the data relate. This may or may not include transparency about what profiles a person's data points match, even if these data points do not count as personal data (because they are merely attributes, not easily linkable to a unique identifier).
29. Bus *et al.* (2013).
30. Which will allow people to contest a restrictive interpretation.
31. Hildebrandt (2008).
32. Agre *et al.* (2001, p. 7).

or not having a certain diploma, having enough credit), unnecessary dissemination of personal data is prevented. One of the drawbacks of this way of proceeding is that people can then be profiled on the basis of their attributes; though they may be anonymous they may still be targeted, since Big Data allows inferences from the usage of such attributes. Another drawback may be that service providers will need proof that the claimed attribute is indeed a 'true' attribute of that person, requiring a link with a root identity that is a real or true identity. Especially in situations where no such link is currently required, this could increase constraints on identity construction based on personalised profiling.

Monetising one's personal data

Some forms of PDM actually strive to enable the monetisation of personal data by the data subject herself. This is interesting because it simply acknowledges that personal and other data are currently monetised, and accepts that this has consequences for those to whom the data relate or to whom data derivatives are applied.[33] Instead of struggling against monetisation, it embraces the idea that this might create added value, but it also demands that those whose data are used as a resource get a share of the profits (Novotny *et al.*, 2013). We could apply Rawls' maximin principle here:[34] whoever manages to create added value is entitled to a bigger share of the cake, as long as the least advantaged do not see their share diminished. This is a way to achieve distributive justice. It is based on the idea that if we all share the same cake, distribution should in principle be equal, whereas anybody who enlarges the cake may claim a slightly bigger share in order to incentivise such an enlargement. The side constraint with the maximin principle is that this may never disadvantage those with the smallest shares and basically requires they be better off too (or at least retain their original share). So, PDM should not create asymmetries that make us – citizens, consumers – worse off in terms of our share of the monetary value than before the advent of Big Data analytics. This would entail engaging us in the monetisation and allowing us to gain part of the profit. It also sustains the incentive to invent applications for Big Data analytics because whoever creates added value gets a good share of the profits.

Obviously there are other types of reasons to engage citizens and consumers in the creation of added value: it should enhance our autonomy, allow us to figure out how we can influence autonomic decision systems and compensate for the knowledge asymmetries that would otherwise subsist. In short, it should reinstate the system of checks and balances that is constitutive for the Rule of Law, thus in a way reinventing the Rule of Law in the era of Big Data – and not merely in relation to the government, but also in relation to other big players that may be more powerful than a government. However, there are also major concerns with PDM systems that allow data subjects to monetise their personal data. The main question is to what extent PDM may simply be co-opted by the industry and government agencies to further monetise our data, precisely by involving our initiative.[35] For instance, what happens if we can foresee what behaviours will increase the monetary value of our behavioural, observed data? What comes from the awareness that we can make money by matching those inferred profiles that turn us into profitable entities? When shall we start reading specific content just because it enables monetisation, instead of reading content that is of no interest to the data brokers, advertising networks and viral marketeers of the Big Data era? Are we going to be influenced by the automated micro-payments that will accompany our machine-readable behaviours? Will this turn us – the observed clusters of data points – into slaves of Big Data?

3. Purpose binding in the era of Big Data

Before answering the question of Big Data slavery, I will investigate one of the core principles of data protection legislation that is under extreme pressure to give way to a more lenient approach to data usage. This concerns the principle of purpose binding, which entails two interconnected rules: (1) the processing of personal data is only allowed for explicit and specific purposes and (2) further processing is not allowed if the purpose no longer applies, unless another purpose that is not incompatible with the original purpose applies.[36] Purpose binding is deeply entwined with the notion of minimal disclosure or data minimisation: once the

33. Hildebrandt *et al*. (2013).
34. Rawls (2005).
35. Thus applying a kind of self-censure on our own behaviours, cf. Hutton *et al.* (1988).
36. Art. 6b, c, d, e of D 95/46/EC and art. 5b, c, d, e and 6(4) of the proposed GDPR.

purpose no longer holds, processing becomes unlawful *even if there was consent*. Under current legislation, in the EU a person cannot waive her right to compliance with purpose limitation, because whatever ground applies (art. 7 DPD) all the conditions of lawful processing apply (art. 6 DPD). In the case of consent (one of the grounds of art. 7), purpose limitation applies (art. 7.a). My questions in this contribution are, how does this principle relate to the 'n = all' of Big Data, and how does it relate to the PDM-type of solutions? More specifically, how does purpose binding relate to contextual integrity, Helen Nissenbaum's salient proposal to rethink privacy and data protection in an era where the opposition between the private and the public spheres is way too coarse to do the work?[37]

Purpose binding and 'n = all'

To the extent that Big Data enables to 'do on a large scale what cannot be done on a smaller scale', purpose binding seems at odds with the business case for Big Data. Big Data wants n, nothing less. Data minimisation, e.g. enabled by attribute-based credentials (ABC) technologies, means that you reduce the data points that are provided (volunteered or observed data) to those necessary for the purpose of processing. For instance, instead of giving your ID to prove your age when buying alcohol, you just claim that you are over 18 and provide the necessary proof without revealing other data points (e.g. your precise age, male or female, etc.). Data minimisation also means that instead of allowing third parties to track your clickstream behaviours across different websites, you eg. only allow the websites you visit to observe behaviours necessary for the technical and functional operations of the website. The purpose of the processing of observed data is then limited to what is necessary for a smooth user experience within the domain of your attention. However, what if observed data are mined to serve the legitimate interest of the advertising network that is tracing and tracking you? What if the explicit and specific purpose of Google Adwords is to create added value for both the advertiser and the website that offers space to auction ads based on behavioural advertising? What if governmental departments decide to reuse data on the basis of a new legal obligation, thus sparing citizens the boring task of providing the same data time and again? Can data collected for billing of energy usage be used for fraud detection if the fraud concerns social security? Can a legal obligation for smart grid operators to provide data for purposes of law enforcement overrule the principle of purpose binding? The 'n = all' of fraud detection implies a business case for having ever more data points on citizens, correlating e.g. energy usage, mobility, location and telecom traffic data to fraudulent behaviours. What was the logic of art. 6(4) of an earlier version of the proposed General Data Protection Regulation that stipulates that:

> Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

Would this mean that, contrary to current law, one could consent to reuse data for an incompatible purpose? Or could governments create new 'legal obligations' to reuse personal data, or claim that reuse is necessary and proportional 'to perform a task carried out in the public interest'? Would this have been this a good way to render data protection compatible with the possibilities to create added value in the Big Data era? Art. 29 WP opined this erodes both data minimisation and purpose binding, because consent means so little in times of cognitive overload, and new legal obligations should not automatically justify reuse.[38] On the other hand, if Big Data is of interest because it generates patterns we could not have foreseen and thus enables usage that could not be predicted, then purpose binding is presumptuous and starts from the wrong premise. We do not know in advance what use is made possible, and to find out we must first mine the data, and to figure out which data are relevant we must mine as much data as possible ('n = all'). The value of Big Data can only be set free if we admit the novelty of the inferred knowledge and rethink purpose binding in line with the innovative potential of its outcomes.[39]

If PDM is the solution, what was the problem?

Let us investigate this by checking whether PDM can be combined with purpose binding. PDM means that a person

37. Nissenbaum (2010).
38. Art. 29 WP Opinion 03/2013, WP203 on the principle of purpose binding, at 38.
39. Massiello *et al*. (2010, pp. 119-124).

has adequate access to and control over where, when and how her own data are being processed. And perhaps also for what purpose, though that is not obvious. If PDM merely allows to grant access and to have information on what entity is using the data, this does not help with enabling purpose limitation. To achieve such a thing would require the privacy policy, the terms of service or the user license agreement to be checked in advance and to trust that the data controller will stick to it. Alternatively, it would require ensuring that the data travel around with a backpack of metadata that determine their legitimate usage, including the terms of their deletion (e.g. self-executing whenever certain conditions apply). Preferably this backpack should enable some form of machine-to-machine reporting on what is going on, while PDM could for instance have a control panel or dashboard that enables targeted destruction of individual data streams if usage is found to be unlawful or – in the case of processing on the basis of consent – if usage is no longer desirable (withdrawal of consent).

However, if we look at the incentive structure of Big Data analytics, we are again confronted with the notion of 'n = all'. PDM may be used to facilitate the mining of as much personal data as possible. Notably, if PDM is designed in a way that gives you a share in the monetisation of your data points, your PDM dashboard may become a play station that generates real income. You can learn to switch data streams to generate the largest profits and you can manage your data in a way that provides you with free access to most of the services. Or can you? Maybe you can manipulate the data streams – of your observed, behavioural data – such that they match profitable profiles. You can learn to game the system. And, of course, some will try to hack your data streams to gain illegal access to your profits. But switching data streams and changing behavioural data patterns probably implies changing your behaviours. Do we really want to tune our machine-readable behaviours to engines of commercial exploitation – and is it really us who will be doing the exploitation once PDM systems are in place? Or will those who offer us money be nudging us into compliant behaviours (compliant with whatever those willing to pay for our data have in mind for us). Will anything we do be measured, stored and mined to make us more nudgeable, more compliant and more foreseeable?

What problem, then, does PDM solve? Does it allow us the illusion of being in charge of our own data points, thus inviting us to collaborate in our own subversion? Are we in the last stages of becoming a composite of commodified and commodifiable data points, a cognitive resource for the intelligent computing systems that manage our external environments, critical infrastructures, income redistribution systems (called taxation), and of the upcoming infrastructure of distributed 3D printing? Is the knowledge asymmetry between the end users, on the one hand, and the companies, the engineers and the designers of distributed interconnected personal data processing systems, on the other hand, not already so extensive that the sheer idea of regaining control betrays a fundamental misunderstanding of the extent to which we are already under control (their control)? For now, I propose that we do not get carried away by techno-pessimism, though I will return to this point in the last part of this contribution.

Purpose binding and contextual integrity

Before that, I will briefly investigate the link between purpose binding and contextual integrity. Both concern the idea that legitimate expectations about the sharing of data partly depend on the role of the data controller (is it your doctor, the NSA or Facebook?), the purpose of processing (is it improving your health, preventing terrorist attacks or increasing shareholder value?) and the context (are we talking about medical advice, safety and security, or commerce?). The difference is that purpose binding requires prior articulation of specific, explicit and legitimate purposes that bind and thus restrict the further processing of personal data. Contextual integrity seems *more vague*, on the one hand, not necessarily requiring prior determination of explicit and specific goals, and *more precise*, on the other hand, making legitimate processing dependent on the legitimate expectations that go with a specific context, independent of explicit articulations of specific purposes. Another difference is that the purpose limitation principle is applicable to individual personal data, whereas contextual integrity applies to data flows. The first is a legal obligation that applies to data processing within EU jurisdictions; the second is an ethical principle, developed within the US by an ethical scholar, Helen Nissenbaum[40] and incorporated in the Consumer Privacy Bill of Rights declared by the Obama administration (without binding

40. Nissenbaum (2010).

force, however, and obviously not meant to be applicable to the NSA).[41] Contextual integrity is especially relevant in the US because of the so-called third-party doctrine that holds that once data have been provided to another party they are considered public and can be shared by that other party with e.g. law enforcement, unless stipulated otherwise in the relevant contract, privacy policy or statute. Purpose binding may rely too much on the old idea that it is possible and sensible to decide on the purpose of data processing beforehand, whereas the added value of Big Data partly resides in the potential to uncover new purposes that may create a win-win situation. Contextual integrity, however, could restrict database fusion, prohibiting the usage of data in a context that is not consistent with the context in which it was collected. Just like in the case of purpose binding, this raises the issue of the added value of unexpected findings in cross-contextual data mining; findings that may generate new medical cures, better prediction of terrorist intention, or more diverse consumer choice?

Purpose binding, as well as contextual integrity, challenges the business case for Big Data. Can we have our cake and eat it too? To figure this out, we need to analyse the dangers of re-use of the same data for a different purpose, e.g. after consent or based on a legal competence, as well as the dangers of cross-contextual data mining. These dangers can be summed up as those of a surveillance society, where the surveillance may be done by the government but also by commercial enterprise and the biggest threats come from where the two sit down to exchange their data. Both the NSA tapping into the metadata of large Internet companies, and science and commerce nourishing on Open Data, increase the 'n = all' conundrum and allow for the use of refined data derivatives to achieve frightful illusions of omniscience. In the next section, I will return to what is actually the problem with this 'n = all' type of illusionary omniscience. Here I would claim that: no, we cannot always have our cake and eat it too. Sometimes we can; sometimes we cannot. It all depends. But if we cannot, we must invent ways to prevent ourselves from being lured into sharing our data points in exchange for instant satisfaction or immediate rewards. Though behavioural economics is somewhat shallow in its analysis of interaction, it confirms the old myth of Odysseus and the Cyrens. Since we seem to have a preference for immediate satisfaction over and above later rewards, we need to build protection into our environments, helping to keep us on course. Requiring prior determination of the purpose of processing may be one way to prevent overly enthusiastic data harvesting, and as a legal stipulation it may have more force than an ethical principle to stick to context.

Now, let us return to the question of who we might become as individuals and as a society with increasing dependence on Big Data infrastructures. This should help us to assess whether prior purpose specification and use limitation are necessary conditions for developing the kind of personhood and the kind of community we want.

4. Endings: who are we in the era of Big Data?

Auto-complete: nudging people into compliance?

This reintroduces the question of the impact of Big Data analytics on our mind, self and society. Morozov has nicely summarised the drawbacks of the imagined omniscience ('n = all'), combined with the solutionist mindset of Silicon Valley's geeks. In his latest book he reminds us that:

> [i]mperfection, ambiguity, opacity, disorder, and the opportunity to err, to sin, to do the wrong thing: all of these are constitutive of human freedom, and any concentrated attempt to root them out will root out that freedom as well.[42]

Legal philosopher Roger Brownsword actually argued similarly with regard to techno-legal solutionism:[43] if technologies enable us to enforce compliance, we are no longer in the realm of law. To qualify as law, we need the right to disobey the law, to challenge its validity in view of higher legal norms and to contest its application in particular instances. The checks and balances of the Rule of Law and the division of tasks between legislator, administration and the courts imply that law appeals to reason and is not set in stone. Whenever technologies enforce compliance, we are in the realm of administration or discipline. If Big Data allows a persistent subliminal pre-emption of our intent, if it autocompletes our environments on the basis of inferred

41. See: <http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>.
42. Morozov (2013, p. xiv).
43. Brownsword (2005, pp. 1-22).

preferences and enables the kind of calculated nudging that will turn us all into law-abiding, friendly, healthy and productive fellows, we should shrink back and reconsider.

So, we should not be fooled by techno-optimists who may have their own reasons to nudge us into auto-completion. But neither should we be overly impressed by techno-pessimists who announce the end of times. Though it is correct to observe that at the moment we are fair game for smart environments that entice us to turn ourselves inside-out while becoming addicted to the latest app, it is also correct to observe that we learn. Just like machines that run the code of the latest form of artificial intelligence, we learn. The question is what we stand to learn here. As indicated above, the bottom line is that we must invent ways to anticipate how smart environments anticipate us, to guess how we are being read, to figure out what *current futures* are inferred and how they will influence our *future currency*. Because whereas machines can develop many *present futures* (predictions of our future behaviours), there will be only one *future present*. To come to terms with smart, data-driven environments we must learn how to outsmart them, to stay one step ahead of them while they try to stay one step ahead of us. This may sound exhausting, but it need not be. On the contrary, it is where we come from and what we cherish in human society: the reiteration of a mutual double anticipation.

A double contingency of Human-Machine Interaction?

Sociologists have called this the 'double contingency' of human interaction.[44] It is what constitutes both human society and individual selves. It is what makes for uncertainty about whether we mean the same thing when referring to the same word, pressing us for techniques and technologies that stabilise meaning despite its inherent instability. Double contingency means that I need to anticipate how you will understand me to be able to make sense. Mead called this 'taking the role of the other', imagining how another sees us; thus being born as a person and developing a sense of self.[45] When I tell a young child: 'you are Sally' while pointing to her, and 'I am Mireille' while pointing to myself, the child will repeat: 'you Sally' while pointing to herself, and 'I Mireille' while pointing to me. I will correct her, but she will be surprised, repeating both the gesture and the name. The moment that Sally understands that to me she is 'you', while to herself she is 'I', she is born again, capable of *taking the perspective of another to herself*. She is now capable of reinventing herself, predicting herself, reflecting on her self, provoking expectations of her self and, ultimately, being provocative by violating those expectations. This is where both our sense of humour and our sense of human freedom emerge. Such freedom cannot be reduced to consumer choice or to freedom from external constraints, it is tied up with the ability to re-view oneself and change course, based on how we foresee that our actions will be interpreted. And all this is made possible by taking the perspective of another. This is why Ricoeur spoke of *Oneself as another*.[46] This is also why Zizek remarked that 'communication is a successful misunderstanding';[47] not just any misunderstanding, but one that succeeds. In what? In nourishing the productive ambiguity of human language, allowing us to act in concert despite recurrent shifts in meaning. In generating new meaning from the interstices of unintended misunderstandings, thus opening the floodgates for new ways of seeing the same things, which thus become other things, allowing us to play around with the implications of our actions, re-viewing them with new eyes – those of other others.

What happens (1) if it is now machines that anticipate us, and what happens (2) if we begin to anticipate how these profiling machines anticipate us? It seems that to 'come into one's own' in a smart environment we have to take the perspective of the inference machines. While the machines are trying to figure us out, we will try to game the system and decide for ourselves whether we are indeed the type of person they have calculated. If PDM enables us to guess the value of our personal data, the double contingency may be reinstated. We might then develop the technologically mediated capacity to guess how we are predicted and learn how to pre-empt the pre-emption of our intentions. That sounds good. There are, however, three caveats here:

The first relates to the question of what happens if machines anticipate us. We should admit that they can only take into

44. Vanderstraeten (1995).
45. George Herbert Mead *et al.* (1962).
46. Ricoeur (1992).
47. Zizek (1991), above nt. 10.

account machine-readable data, and their inferences are contingent on a population consisting of machine-readable data. N, therefore, cannot be All, because not everything can be discretised. Datafication is both a multiplication of reality, a virtualisation in the sense of Deleuze,[48] and a reduction of reality, because it necessarily translates the flux of life into discrete data points. This is the same for written language, by the way. But written language is visible for those who learned to read and write, whereas computer language is the secret knowledge of the experts.

The second relates to the question of what happens to us if we begin to anticipate these machines. Shall we, in figuring out how machines 'think', become more like machines and lose some of the ambiguity inherent in the usage of spoken and written language? Is Brian Christian right that instead of machines becoming more like humans, we are becoming more like machines?[49] Is Maryanne Wolf right that the morphology and the behaviour of our brains will change and that we must ask what must be preserved, highlighting that we cannot take for granted that our brains will adapt without losing what was developed in the course of our evolution as reading animals?[50]

The third relates to the transparency that reinstates the double contingency. The PDM model, described earlier, may enable intuitive transparency by means of monetisation. The introduction of a *tertium comparationis* in the form of money – of a price – could empower us to foresee how our data points match inferred behavioural models. But, as we have seen above, this may create perverse incentives. The question is, however, whether we have alternatives.

Currently, the transparency that is provided whenever prior informed consent is required creates a 'buffer overflow': the amount of information it involves floods our bounded rationality and this enables manipulation by what escapes our attention. Though some would applaud the Enlightenment of Descartes' *idées claires et distinctes*, others may point out that they generate overexposure, wrongly suggesting the possibility of light without shadows. The metaphor of the buffer overflow actually suggests that we may require selective enlightenment, and that we are in dire need of shadows. The more interesting question, therefore, will be what should be in the limelight and where do we need darkness. In Renaissance painting, the techniques of the *claire-obscure*, the *chiaroscuro*, the *Helldunkel* were invented and applied to suggest depth, and to illuminate what was meant to stand out. By playing with light and shadow, the painting could draw the attention of the onlooker, creating the peculiar experience of being drawn into the painting – as if one is standing in the dark, attracted by the light. Big Data analytics invites us to reinvent something like a *claire-obscure*, a measure of transparency that enables us to foresee what we are 'in for'. This should enable us to contest how we are being clustered, correlated, framed and read, thus providing the prerequisites for due process. This should, finally, enable us to play around with our digital shadows, acquiring the level of fluency that we have learned to achieve in language and writing.[51]

I end this contribution with a reference to the enigma of the Sphinx on the cover of a book I recently co-edited with Katja de Vries. It depicts Oedipus in the *clearing* of a *clair-obscure*. He stands out strong, wilful and looks somewhat impatient. The Sphinx stands in the shadow of a cave, potentially irritated that a trespasser has finally solved her riddle. However, though Oedipus may have solved the riddle, he cannot evade the fundamental fragility it foretells. Though monetisation of personal data points may help to reinvent a new version of the double contingency that constitutes our world, it cannot resolve the fundamental uncertainty that it sustains. In fact we need transparency tools that help to reinstate this uncertainty, rather than the over-determination that monetisation might otherwise enable.

48. Deleuze (1994); Lévy (1998).
49. Christian (2011).
50. Wolf (2008).
51. This and the next paragraph - literally - draw on Hildebrandt (2013b, pp. 238-9 and 241).

References

AARTS, Emile; MARZANO, Stefano (2005). *The New Everyday. Views on Ambient Intelligence*. Rotterdam: 010, 2003. ITU. "The Internet of Things". Geneva: International Telecommunications Union (ITU).

AGRE, Philip E.; ROTENBERG, Marc (2001). *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts: MIT, p. 7.

AMOORE, Louise (2011). "Data Derivatives on the Emergence of a Security Risk Calculus for Our Times". *Theory, Culture & Society,* vol. 28, iss. 6, pp. 24–43.

ANDERSON, Chris (2008). "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete". *Wired Magazine,* vol. 16, iss. 7.

BOYD, Danah; CRAWFORD, Kate (2012). "Critical Questions for Big Data". *Information, Communication & Society*, vol. 5, iss. 4, pp. 662–679, http://dx.doi.org/10.1080/1369118X.2012.678878.

BROWNSWORD, Roger (2005). "Code, control, and choice: why East is East and West is West." *Legal Studies,* vol. 25, iss. 1, pp. 1–22. http://dx.doi.org/10.1111/j.1748-121X.2005.tb00268.x.

BUS, Jacques; NGUYEN, Carolyn (2013). "Personal Data Management – A Structured Discussion". In: Mireille HILDEBRANDT, Kieron O'HARA, Michael WAIDNER (eds.) *The Value of Personal Data. Digital Enlightenment Yearbook 2013*. Amsterdam: IOS Press.

CHOPRA, Paras (2010). "The Ultimate Guide To A/B Testing". *Smashing Magazine*. <http://www.smashingmagazine.com/2010/06/24/the-ultimate-guide-to-a-b-testing/.>

CHRISTIAN, Brian (2011). *The Most Human Human. What Talking with Computers Teaches Us About What It Means to Be Alive*. New York: Doubleday.

DAVIDSON, Joe (2013). "NSA to cut 90 percent of systems administrators. Federal Eye". In: *Washington Post*. 13th August 2013, available at: <http://www.washingtonpost.com/blogs/federal-eye/wp/2013/08/13/nsa-to-cut-90-percent-of-systems-administrators/>

DE HERT, Paul; GUTWIRTH, Serge (2006). "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power". In: Erik CLAES, Antony DUFF, Serge GUTWIRTH (eds.). *Privacy and the Criminal Law*. Antwerpen Oxford: Intersentia.

DELEUZE, Gilles (1994). *Difference and repetition*. New York: Columbia University Press.

ESPOSITO, Elena (2011). *The Future of Futures: The Time of Money in Financing and Society*. Edward Elgar.

GITELMAN, Lisa (ed.) (2013). *'Raw data' is an oxymoron*. Cambridge, MA – London, England: MIT Press.

FAYYAD, Usama M.; PIATETSKY-SHAPIRO, Gregory; SMYTH, Padhraic [*et al.*] (1996). *Advances in Knowledge Discovery and Data Mining*. Meno Park, CA - Cambridge, MA - London England: AAAI Press / MIT Press, p. 41.

FLORIDI, Luciano; SANDERS, J.W. (2004). "On the Morality of Artificial Agents". *Minds and Machines, vol.* 14, iss. 3, pp. 349–379. http://dx.doi.org/10.1023/B:MIND.0000035461.63578.9d.

HILDEBRANDT, Mireille (2013a). *Legal Protection by Design in the Smart Grid*. Report, assigned by the Smart Energy Collective. Nijmegen/Groningen. <http://works.bepress.com/mireille_hildebrandt/42/>.

HILDEBRANDT, Mireille (2013b). "Profile Transparency by Design: Re-enabling Double Contingency". In: M. HILDEBRANDT, E. DE VRIES (eds.). *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Abingdon: Routledge, pp. 238-9.

HILDEBRANDT, Mireille (2012). "The Dawn of a Critical Transparency Right for the Profiling Era". In: *Digital Enlightenment Yearbook 2012*. Amsterdam: IOS Press, pp. 41–56.

HILDEBRANDT, M. (2008). "Profiling and the identity of the European citizen". In: M. HILDEBRANDT, S. GUTWIRTH (eds.). *Profiling the European citizen. Cross-discplinary perspectives*. Dordrecht: Springer. http://dx.doi.org/10.1007/978-1-4020-6914-7.

HILDEBRANDT, M.; O'HARA, K.; WAIDNER, M. (2013). *The Value of Personal Data. Digital Enlightenment Yearbook 2013.* Amsterdam: IOS.

HORNUNG, G.; SCHNABEL, Ch. (2009). "Data protection in Germany I: The Population census decision and the right to informational self-determination". *Computer Law & Security Reports,* iss. 1, pp. 84-88. http://dx.doi.org/10.1016/j.clsr.2008.11.002.

HUTTON, Patrick H.; GUTMAN, Huck; MARTIN, Luther H. [*et al.*] (1988). *Technologies of the self: a seminar with Michel Foucault*. Amherst: University of Massachusetts Press.

KEPHART, Jeffrey O.; CHESS, David M. (2003). "The Vision of Autonomic Computing". *Computer*. January, pp. 41-50. http://dx.doi.org/10.1109/MC.2003.1160055.

KOHAVI, Ron; HENNE, Randal M.; SOMMERFIELD, Dan (2007). "Practical guide to controlled experiments on the web: listen to your customers not to the hippo". In: *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*. New York, NY: ACM, pp. 959-967. http://dx.doi.org/10.1145/1281192.1281295.

LÉVY, Pierre (1998). *Becoming Virtual. Reality in the Digital Age*. New York and London: Plenum Trade.

LUHMANN, Niklas (1995). *Social Systems*. Stanford: Stanford University Press.

MASSIELLO, Betsy; WHITTEN, Alma (2010). "Engineering Privacy in an Age of Information Abundance". In: *Intelligent Information Privacy Management*. AAAI, pp. 119-124.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth (2013). *Big data: a revolution that will transform how we live, work and think*. Boston: Houghton Mifflin Harcourt, p. 6.

MCSTAY, Andrew (2011). *The mood of information: a critique of online behavioural advertising*. New York: Continuum, p. 3.

MEAD, George Herbert; MORRIS, Charles William (1962). *Mind, self, and society from the standpoint of a social behaviorist*. Chicago: University of Chicago Press.

MERTON, Robert K (1948). "The Self-Fulfilling Prophecy". *The Antioch Review*, vol. 8, iss. 2, pp. 193-210. http://dx.doi.org/10.2307/4609267.

MITCHELL, Tom M. (2006). "Introduction". *The Discipline of Machine Learning*. Carnegie Mellon University, School of Computer Science.
‹http://www-cgi.cs.cmu.edu/~tom/pubs/MachineLearningTR.pdf›.

MOROZOV, Evgeny (2013). *To save everything, click here: the folly of technological solutionism*. New York: Public Affairs, p. xiv.

NISSENBAUM, Helen (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.

NOVOTNY, Alexander; SPIEKERMANN, Sarah (2013) "Personal Information Markets and Privacy: A New Model to Solve the Controversy". *WI'2013.* Leipzig. ‹http://ssrn.com/abstract=2148885›
‹http://dx.doi.org/10.2139/ssrn.2148885 ›

PEIRCE, Charles Saunders (1958). *Selected Writings, edited with an introduction and notes by Philip P. Wiener*. New York: Dover.

RAWLS, John (2005). *A theory of justice*. Cambridge, MA: Belknap Press.

RICOEUR, Paul (1992). *Oneself as Another*. Chicago: The University of Chicago Press.

ROUVROY, A.; POULLET, Yves (2009). "The right to informational self-determination and the value of

self-development. Reassessing the importance of privacy for democracy". In: S. GUTWIRTH, P. DE HERT, Y. POULLET (eds.) *Reinventing Data Protection*. Dordrecht: Springer.

RUSSELL, Stuart J.; NORVIG, Peter; DAVIS, Ernest (2010). *Artificial intelligence: a modern approach*. Upper Saddle River, NJ: Prentice Hall.

STENGERS, Isabelle (1997). *Sciences et pouvoirs*. Paris: La Découverte, pp. 62-63.

VAN DEN BERG, Bibi (2010). *The Situated Self: Identity in a world of Ambient Intelligence*. Nijmegen: Wolf Legal Publishers.

VANDERSTRAETEN, R. (2007). "Parsons, Luhmann and the Theorem of Double Contingency". *Journal of Classical Sociology,* vol. 2, iss. 1, pp. 77–92.

WOLF, Maryanne (2008). *Proust and the Squid: The Story and Science of the Reading Brain*. Icon Books Ltd.

WORLD ECONOMIC FORUM (2011). *Rethinking Personal Data: Strengthening Trust*. ‹http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf›

WORLD ECONOMIC FORUM (2013). *Rethinking Personal Data: Unlocking the Value of Personal Data: From Collection to Usage*. ‹http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage›

ZIZEK, Slavoj (1991). *Looking awry: an introduction to Jacques Lacan through popular culture*. Cambridge, MA: MIT Press, p. 30.

Recommended citation

HILDEBRANDT, Mireille (2013). "Slaves to Big Data. Or Are We?". *IDP. Journal promoted by the Law and Political Science Department*. No. 17, pp. 27-44. UOC. [Accessed: dd/mm/yy]
http://journals.uoc.edu/index.php/idp/article/view/n17-hildebrandt/n17-hildebrandt-en
http://dx.doi.org/10.7238/idp.v0i17.1977

About the author

Mireille Hildebrandt
Chair of Smart Environments, Data Protection and the Rule of Law
Institute for Computing and Information Sciences (iCIS)
Radboud University Nijmegen
hildebrandt@law.eur.nl

Mireille Hildebrandt started her academic life with a taste of cultural anthropology, later switching to law. She took her law degree from Leyden University in the Netherlands and defended her PhD thesis in the philosophy of criminal law at Erasmus University Rotterdam, integrating legal anthropology and legal history to develop a hermeneutic phenomenology of punishment.

Presently she holds the chair of Smart Environments, Data Protection and the Rule of Law at the Institute for Computing and Information Sciences (iCIS) at Radboud University Nijmegen. She is Associate Professor of Jurisprudence at the Erasmus School of Law and since 2002 she has been seconded part-time to the Centre for Law Science Technology and Society (LSTS) at Vrije Universiteit Brussels. Her research interests concern the relationship between the emerging socio-technical infrastructure (Internet, Web 2.0, Ambient Intelligence) and the autonomy of the human subject that is both presumed and produced by constitutional democracy. Together with Serge Gutwirth she edited 'Profiling the European Citizen' (Springer 2008) and with Antoinette Rouvroy 'Law, Human Agency and Autonomic Computing' (Routledge 2011).

Personal webpage: <http://works.bepress.com/mireille_hildebrandt/>

Faculty of Science
University of Nijmegen
Postbus 9010
6500GL Nijmegen
The Netherlands