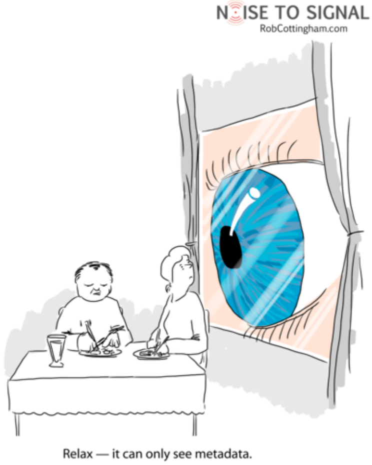
Digital Enlightenment Yearbook 2013
M. Hildebrandt et al. (Eds.)
IOS Press, 2013
© 2013 The authors.
doi:10.3233/978-1-61499-295-0-1

Introduction

Mireille HILDEBRANDT[a,1], Kieron O'HARA[b] and Michael WAIDNER[c]
[a] *Radboud University Nijmegen, Vrije Universiteit Brussel,*
Erasmus University Rotterdam
[b] *University of Southampton*
[c] *Technische Universität Darmstadt*

Keywords. Personal data management, privacy, privacy by design, personal data ecosystems, Enlightenment



If you have nothing to hide[2]

1. *Was Ist Aufklärung* in the Age of Personal Data Monetisation?

1.1. Enlightenment

The 18th century Enlightenment thinkers inspired new relationships with knowledge, power, authority and human values. Critical thought, balancing of countervailing powers, rejection of un-scrutinised or unaccountable authority and a strong emphasis on human autonomy and individual flourishing are often heralded as the unassailable heritage of western civilization. The narratives of empiricism (Bacon), scepticism (Hume), rationalism (Descartes, Voltaire, Kant) and epistemological inquiry (Kant again), as well as theological, political and ethical radicalism (Spinoza) have shaped the course of

[1] Corresponding Author.

[2] Reproduced with permission from Rob Cottingham. See http://www.robcottingham.ca/cartoon/archive/if-you-have-nothing-to-hide/.

western traditions and even evoked forms of Enlightenment fundamentalism. Without denying the many contradictions and inconsistencies between different strands of Enlightenment thought, the *Digital Enlightenment Forum* aims to build on the historical artefacts of critical thinking (daring to contest mainstream knowledge claims), countervailing powers (speaking truth to power), transparent government (as a precondition for accountability) and the protection of civil liberties (as a precondition for individual autonomy and political participation). These values cannot be taken for granted, and are confronted with novel challenges in the era of Big Data and information-driven government, commerce and science.[3] The proliferation of incredibly massive searchable datasets, the increasing use of predictive analytics in almost every domain of public and private life and the extent to which critical infrastructure has come to depend on information and communication technologies (ICTs), warrant a new Enlightenment discourse to sustain the values we want to preserve and/or need to reinvent. The Age of Reason seems to slip into the Age of the Algorithm, the Age of Correlation or the Age of Data-Driven Nudging. As Bateson, one of the founding fathers of cybernetics, would say: what is the difference that makes a difference here [1, p. 315]? How to reclaim the patience, the prudence, the practical wisdom and the reflective equilibrium that nourished the Rule of Law, in the era of hyper-connectivity and real time autonomic decision systems? To put it more bluntly in terms of the subject matter of this volume: *Was ist Aufklärung* in the Age of Personal Data Monetisation?

1.2. The Dialectic of Digital Enlightenment

Enlightenment remains an important reference point for the enquiries reported in this volume. The Enlightenment era, firmly rooted in the information infrastructure of the printed word, nourished the practices of systemisation, indexing and codification, as Bernard Stiegler argues in this volume. Our political, business and legal systems are rooted in Enlightenment concepts such as enforceable rights, individualism and the power of reason. In this world, privacy plays several important roles, protecting the autonomy of individuals and governing their relationships with institutions, communities and society as a whole.

The advent of digital computing systems, networking, data mining and machine learning, is in tension with those concepts, while consistent with the idea of rationalistic mastery over our environment, which is often associated with Enlightenment thought (notably that of Francis Bacon). This tension is an example of how specific Enlightenment ideals initiate a dialectic where their very success threatens their foundations, as Adorno and Horkheimer famously argued [2] (and see also [3]). The paradigmatic anti-Enlightenment philosopher Nietzsche framed the dialectic of Enlightenment in a characteristically pithy way, which still reflects our own ambivalence. Enlightenment, for Nietszche, releases the individual from domination: “the priests all become priests with a bad conscience – and the same must be done with regard to the State. That is the task of the Enlightenment: to make princes and statesmen unmistakeably aware that everything they do is sheer falsehood”. Equally, he saw, in Enlightenment’s promise of non-domination, a tool for manipulation. “The way in which the masses are fooled in this respect, for instance in all democracies, is very useful: the

[3] Big data is of course not the only novel and challenging factor. We could also cite, for instance, global connectivity, the Internet of Things, online social networks, and cloud computing.

reduction and malleability of men are worked for as 'progress'!"[4] This dialectic shows itself today by the very control over our data that the Digital Enlightenment affords,[5] creating a resource of great value for governments and corporations who thus impose their own ideas of our well-being upon us, potentially manipulating and even removing our autonomy.

Dynamic interconnected networks of individuals, private and public organisations, identities, credentials, personal and other data often demand massive and real time processing. Yet our social norms also evolve to accommodate these technological developments. The mindset of a digital immigrant seems at odds with that of a digital native [4]. To some, privacy may appear more costly, as it can be traded off for the benefits that follow from being highly visible to the network, while the volume of data available for processing makes it impossible for the individual to police effectively – even though, as Robert Madelin's Foreword to this volume makes abundantly clear, user trust "is key to Big Data success".

There are substantial implications for trust and mutual expectations, as the extent to which individuals are capable of overseeing and foreseeing how their data are processed, shared and put to use by whom, where, and to what purpose is now unclear. Despite that, assumptions from the pre-digital era still govern current policy. It is becoming increasingly hard to track what knowledge is mined from the proliferation of networked data, how such knowledge will map onto individuals' identities, and what consequences will follow from these matches.

The chapters in this yearbook have been invited from not only scholars from across various disciplinary backgrounds, notably computer science, psychology, law and philosophy, but also a number of authors involved in specific personal data management initiatives, and they investigate how these technologies will affect individuals with regard to privacy, informational self-determination, contextual integrity, and the notions of personal identity and the networked self. What *values* do the different stakeholders associate with and derive from personal data and individual privacy? What are the options for individuals and society to *control* the use of personal data in a digital world full of user-generated content, multinational service providers, smart and interconnected devices, and sophisticated Big Data algorithms? How can individuals and civil society organisations use these new technologies for their *own benefit* and for *their own perception of the public benefit*, for example, via the exploitation of open data – and, when it comes to open data, can they really exploit without being exploited? To what extent can increasing *transparency* support trust and privacy? What technical and social infrastructures are needed for supporting control and transparency? Can they be put in place without destroying the social (and commercial) value that Robert Madelin highlights? And what if they can't? To what extent must a Digital Enlightenment live with the monetisation of our personal data?

2. The Value of Personal Data

Though the title of this book speaks of *The Value of Personal Data*, we can no longer take for granted that the concept of value refers to something mental, ethical and in-

[4] These are quotes from his *Nachlass*, his unpublished notebooks.

[5] Though we do not necessarily agree that the proliferation of digital infrastructures can be qualified as a Digital Enlightenment.

valuable. This volume aims to confront the notion of 'values' in the sense of guiding principles for individual persons and their societies with that of 'value' in the sense of monetary value. In the chapters that follow, the incalculable worth of the value of a person and her data is confronted with the quantifiable worth of manipulable,[6] machine-readable data that relate to an identifiable individual person. It thereby builds on a tension that is inherent in the Enlightenment Age, namely between reason and rationality, between what must be argued and what can be calculated. It may be, that to preserve the *invaluable value* of our personhood we need to engage with the *calculable value* of the personal data on which so many business cases in public administration and industry now depend. Monetisation of personal data is already a fact. To reclaim some degree of autonomy as an individual person, society may have to enable a person to anticipate how her data can be monetised and what could be the consequences of 'leaking' her data:[7] loss of a job, lucrative discounts, personalised surveillance, exclusion from social security benefits, rejection of credit, or being registered on whatever blacklist. The point is not so much to provide people with a share of the profits made by the monetisation of personal data, but foremost, the idea is to create effective transparency and control over what data are captured, created, mined and aggregated in order to come to grips with the usage, abuse and exchange of our data.

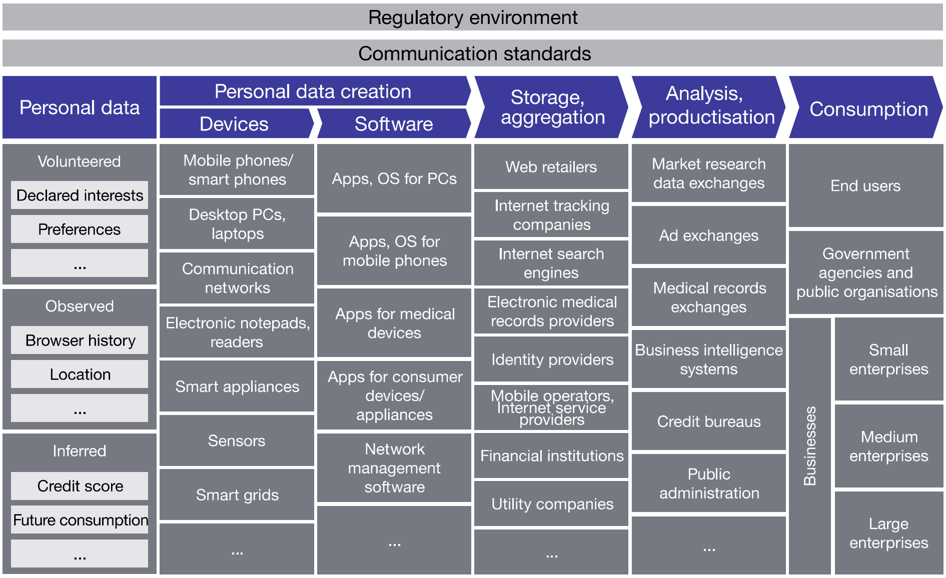
2.1. Volunteered, Observed and Inferred Data

The World Economic Forum (WEF) has initiated a series of discussions under the heading of *Rethinking Personal Data*, notably reporting on personal data as a new economic 'asset class'. In its 2011 report on *Personal Data: The Emergence of a New Asset* [5], the WEF discriminated between three types of data: volunteered, observed and inferred data (see Fig. 1).

Volunteered data are defined as data that individuals "explicitly share about themselves" through electronic media, for example, when someone creates a social network profile or enters credit card information for online purchases. Observed data are data "captured by recording activities of users" (in contrast to data they volunteer). Examples include Internet browsing preferences, location data when using cell phones or telephone usage behaviour. Inferred data are "data from individuals, based on the analysis of personal data [such as] credit scores… calculated based on a number of factors relevant to an individual's financial history". Though the categories may overlap, this mapping of personal data and data that may affect a person is a timely proposal to bring some order in the debate over the sharing of personal and unpersonal data. Obviously, volunteered data are indeed created by a person in the sense of her deciding what information to hand over for whatever reason to whichever other person, organisation or software programme. Observed data, however, are in fact created by the software that tracks and traces our online and offline behaviours: clickstream, public transport, electronic payment, mobility, jogging or any type of machine readable behaviour. These data refer to a specific person, and are therefore personal data under EU data protection legislation, but they are 'made' by the software machines of companies or public administration departments. Inferred data are 'made' by data mining technologies, looking for patterns in the volunteered and/of observed data, that are aggregated

[6] On the meaning of the term manipulation, see Stiegler in this volume.

[7] 'Leaking' refers to what the World Economic Forum calls 'observed' data, they are mostly behavioural data that register clickstream, mobility, purchasing and other data without our conscious or deliberate intention to share such data.



Source: Bain & Company

Figure 1. The Personal Data Ecosystem: A Complex Web From Data Creation to Data Consumption.[8]

in a database. These inferred data need not refer to an identifiable person, as they may be statistical correlations or other patterns, mined from the anonymised data of millions of people. However, the fact that such patterns are not personal data does not mean they will not impact individual persons. Once a subset of data points match such patterns, a person may be identified as one who is willing to pay a higher price, to take more risk, or one who is prone to develop a specific disease or inclined to aggressive behaviour. Though this is all about statistics, the consequences of applying such probabilities to individual users are real. Protection is warranted, even when inferred data are not personal data [6].

2.2. Working Definitions

In this volume, the authors have examined the extent to which privacy and data protection require new technological, legal and organisational architectures in the era of proliferating personal data ecosystems. Since the field we are exploring is an emergent domain of knowledge we will start with a set of explorative definitions, to help the reader to navigate a pioneer's landscape.

The value of personal data. As already mentioned above, the value of personal data can be understood in two ways: as an invaluable asset that is intrinsically linked to the individual person, and as a quantifiable variable that can be traded against various types of services or even money.

Identity. In the context of digital security and data protection, the term identity often refers to either the complete set of attributes that define an individual person or

[8] This figure was taken from [5, p. 15], © World Economic Forum (WEF), Bain Company, and Marc Davis, who developed the concepts of volunteered, observed and inferred data in collaboration with the WEF.

whatever data can uniquely identify a natural person. This can be said to stand for identity in the technical sense, and it relates to identification and authentication. In the context of privacy and human values, identity refers to the sense of self that individuals develop in the course of their lives, enabling them to develop an ‘own’ personality and to act as a moral and legal agent.

Privacy and data protection. The human right of privacy is usually seen as a liberty or negative freedom, i.e. imposing an obligation on others not to interfere with the home, private and family life, and communications of a person. As a liberty, it is not easy to define, as definitions restrict its scope. As a human right, privacy protects against infringements by the state, though horizontal effect may oblige states to protect their citizens against privacy infringements by other citizens or private companies. Data protection is a set of legal norms that more strictly defines a set of rights of data subjects (those to whom personal data relate) and obligations of data controllers (those who determine the purpose of data processing). Privacy rights prohibit infringement of the privacy; data protection conditions the free flow of information. Privacy protects the opacity of the individual; data protection warrants transparency of personal data processing. Though some would claim that consent is the hallmark of data protection, others will argue that informed consent is becoming illusive, and purpose limitation is the main protection offered by data protection legislation.

Personal data ecosystems (PDE). In descriptive terms this concept refers to the interacting personal data processing systems (PDPSs) that have been proliferating for some time now. This may concern the vast data servers that store data collected by the National Security Agency (NSA), or the consumer data aggregated and mined by data brokers such as Axciom or Experian, who sell consumer profiles for marketing or credit rating, or those that offer public or private cloud services to either businesses or individual end users. It may also concern those that offer authentication services (trusted identities in the technical sense) or personal data management services (based on credentials or attributes as pseudonyms). At a higher level of abstraction, a PDE may include Trust Frameworks and Trust Networks that should allow, for example, context-aware personal data management.

Personal data management (PDM). Though PDM is also the acronym for personal data monetisation, we use it to refer to the user-centric management of an individual’s own personal data – facilitated by various types of architectures – to make sure that a person can retain a degree of control over who gets access to which of her personal data. In many ways it builds on user-centric Identity Management Systems. PDM can be achieved by securing one’s personal data in a digital vault (on one’s own device or distributed in a cloud) and the architecture may be offered by one service provider to all of its customers or in the form of a platform which allows individuals to connect in a secure way with various service providers. The bottom line is that a user’s personal data are not shared without their consent, or in the case of necessity (contract, a legal obligation, vital interests, public tasks or the legitimate interests of the data controller), on condition that they will not be used for other purposes than those stipulated when access was provided. Monetisation can be the effect of personal data management, i.e. if companies are willing to share part of the profits they make on the value of personal data with the data subject. PDM may lead to a situation where the added value services which are nourished by personal data will only function if data subjects can actively and knowingly participate in the creation of the added value, while getting their piece of the cake that was thus enlarged. One important issue is to what extent PDMs will provide adequate control over the observed and inferred data that nourish most of the business cases of Big Data analytics.

2.3. User-Centric Personal Data Management

The basic mechanisms that the various authors in this volume explore for understanding and managing this delicately balanced ecosystem are user-centric data management tools; methods and business models that are intended to empower the individual by allowing her a measure of control over her own data. This should not only concern her volunteered but also her observed data and the inferences made from them. User-centric data management is of course only one solution to the problems described above, but it is worth considering as a focus for this enquiry, as it has the potential for addressing the problems while remaining consistent with the Enlightenment project of self-determination. Both within the regulators and within the industry the idea has been taken up to develop some form of personal data management as a follow-up to identity management.

The vision of personal data management is quite simple; the data subject controls and curates data about herself (not all data, but the data she is able to collect). If anyone wants it, they have to ask her for it – she gives them whatever she wants to share. If she wishes to keep the data to herself, then she does not give out information. She can give a certain piece of information to one person (her doctor, say), but not another (her insurance broker). This is a complex process, but it is managed by software tools which simultaneously store or access the data (it may be distributed across various repositories), and manage the interface between data subject and data user. She can outsource the management of the data to other organisations, and ask them to intercede for her; many of the likely situations where her information is required will be too complex for her to want to manage, and the volume of requests may simply outpace her ability to monitor them personally. There are clearly issues of trust, usability and security raised by such an arrangement. Is it feasible? Is it limited to access management or could it also enable usage management? The vision is simple – its implementation is hardly so.

How are we to understand user-centric personal data management? This issue is explored at the theoretical level in the chapter by Bus and Nguyen, who provide an abstract specification of the various relationships and positions relevant to the social and technical context of the new digital world as they impact on the individual and her self-determination. They promote the idea of context-aware personal data management, building on ideas from thinkers such as Kim Cameron and Ann Cavoukian (both represented in this volume) in the following terms: "*Context-aware PDM (CPDM) 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. Trustworthy data practices are foundational to enabling Context-aware PDM.*"

Bus and Nguyen unravel this definitional statement in their chapter, but without anticipating their careful discussion, it is useful for us to highlight a couple of its aspects. It sets out an *ideal* for personal data management in terms familiar to students of the rationalist version of Enlightenment. The ideal technological solution produces autonomy for the individual, in particular, by allowing her to develop her identity (or identities), in the sense of selfhood, and to present different aspects of those identities to different audiences and organisations depending on the requirements of the context and her own preferences (i.e. she identifies herself in a more technical sense). To get a beer she needs to show she is over 18 while to drive a car she needs to show that she has taken an appropriate test, which will clearly require a greater release of information. To access a web service she may be required to accept tracking and tracing, which she could reject by default or accept depending on certain conditions.

This autonomy has limits. For instance, in order for an identity, in the technical sense, to be useful it has to serve the purposes not only of the individual but also of organisations demanding it. The data required to drink a beer, while disclosing minimal information, must be verifiable. This must inevitably stifle some of the individual's options – for example, she may creatively wish to present herself as she is not (for example, to fake some episodes in the past). There are many reasons why this could be done – most obviously determining one's own identity (for example as a good father or mother) is not always strongly connected to the facts. Erving Goffman's dramaturgical analysis of the presentation of the self, by evoking the theatre, *ipso facto* evokes the possibility of creative reconstruction [7]. The function of memory is not the retrieval of facts, but rather sensemaking, which is not dependent on the strict truth of what is remembered. More prosaically, Dodge and Kitchin [8] have argued that the best way to protect personal data stores is to falsify random pieces of information so that anyone snooping in the store cannot be certain that a particular data item retrieved is actually true. Mayer-Schönberger [9] has produced a related argument that the only way to ensure that identities can develop in a non-pathological way is to delete information periodically and automatically. This does somewhat overturn the Enlightenment ideal for personal data management by removing human agency from the decision-making.

There is indeed a flip side to the rationalist version of the Enlightened ideal of personal data management, which is that the collected data, even (perhaps especially) if curated by the data subject herself, is a valuable resource for others. Commercial organisations may pay for the right to process or use it. That at least would allow the individual some rights over how the information is used, but as Hildebrandt has argued [10], without transparency the individual may be unaware of how it will be used and what value will be extracted by the purchasing firm. How can she make an informed decision to provide access? How can her supposed autonomy be reconciled with her profound ignorance of what is likely to happen?

Perhaps more to the point, governments will always give themselves the powers to use collected data, covertly or otherwise [11]. Policing, national security and public health are reasons that will always be cited. And, although one wearies of the extraordinarily dim, wilfully complacent and shockingly bogus argument that "if you have nothing to hide you have nothing to fear," it is routinely trotted out, not only by tabloid newspaper editors with a vested interest in the destruction of privacy, but also by responsible public officials. It was, for instance, the response of the United Kingdom's Foreign Secretary William Hague [12] in a comment about the US government's clandestine PRISM surveillance programme, the existence of which was revealed (a "landmark event", according to Kim Cameron in his Afterword in this volume) by a whistleblower in *The Washington Post* and *The Guardian*. Yet the UK Intelligence Services Act of 1994 allows electronic surveillance "in the interests of the economic wellbeing of the United Kingdom in relation to the actions or intentions of persons outside the British islands", which has allegedly been interpreted as allowing the UK government to bug foreign diplomats to determine their negotiating positions prior to economic summits [13]. These diplomats had something to hide, sure – but it is perfectly legitimate to want to hide a negotiating position.

The PRISM affair highlights an important failing of the European digital economy. European citizens are at risk from American snoopers because there are very few alternatives to US-led online services. We use Google, Facebook and Twitter because the European alternatives are puny in comparison. This is partly due to the first-mover advantage afforded by network effects, but partly it reflects the greater entrepreneurialism evident in Silicon Valley, which has had the unhappy effect of giving the NSA easy access to 'our' data.[9] It is probably a myth that President George W. Bush once declared that the trouble with the French is that they have no word for entrepreneur, but given the US's commercial lead, it has the ring of truth (applied not only to the French, but to Europe as a whole). As demonstrated in this volume, there are plenty of options for the private sector to move into the space of personal data management – and this may be the very time to strike.

The bottom line is simple: if we put all our data eggs in one basket, we should not be surprised when those interested in us make a grab for the basket. Hence we endorse the conclusion of Bus and Nguyen that the functioning of the edifice of personal data management would require appropriate norms, regulations and "trustworthy data practices". To the extent that it provides for data protection by design it might even enable a win-win situation, though if it merely allows consumers to trade their data without inbuilt verification of lawful and fair *usage* it is unclear what the advantage will be. We should not allow ourselves to become compromised by our own involvement in the monetisation of personal data in ways that undo the invaluable value of personal data.

3. Autonomy and Heteronomy in the Era of Predictive Analytics

As philosopher Bernard Stiegler observes, in our first Chapter, '*Die Aufklärung* in the Age of Philosophical Engineering':

> And while traceability continues to expand, it seems it is mainly being used for behaviour profiling, and thus to increase the heteronomy of individuals rather than their autonomy.

The combined usage of volunteered, observed and inferred data that concerns us – because these data refer to us and/or generate all types of automated decisions about us – confronts us with a novel cognitive economy. The quantity, forms and implications of privately held or publicly shared knowledge have long since reached unprecedented levels of accumulation, while no human mind nor any computing system could claim to 'know' the content of all the data 'out anywhere'. Is it important, therefore, to reassess what it means that so much information is being processed by interacting computing systems whose operations are opaque to most of us and may even be hard to assess by those who designed them. Stiegler, in fact, describes how the grammatisation (discretisation) of behaviours follows up on the earlier grammatisation of spoken and written language, all depending on what he identifies as retention, i.e. our ability to retain the flux of life as a perception (primary retention), a memory (secondary reten-

[9] Though having said that, the colossal Tempora programme of the UK's GCHQ to 'Master the Internet' is also stunning in the quantity of data and metadata it amasses, all on the basis of an innocuous loophole in the Regulation of Investigatory Powers Act 2000, which has allowed GCHQ's lawyers to present a case for Tempora's legality, but has also cast doubt on its democratic legitimacy. GCHQ allegedly shares sensitive personal information with the NSA [14].

tion) and by means of technical devices that allow the storing or even the machine-to-machine processing of information (the handwritten manuscript, the printing press, photographs, mass media, and now, the digital computer and the Internet; all different forms of tertiary retention). For a tertiary retention to make sense to us, we need to introject it; to make it 'come to mind' – otherwise it remains outside our cognition and cannot inform our actions. The Enlightenment Age, with its emphasis on critical thinking and reasoned discourse, may be understood as the age of 'reading brain'. As Stiegler indicates, referring to the work of Maryanne Wolf [15], the morphology as well as the behaviour of a 'reading brain' differs substantially from brains that have not been trained to read and write. So, if introjection of written text is a matter of reading, what would be the introjection of Big Data or of predictive analytics – that altogether different tertiary retention? Stiegler thus raises the important question of what politics are involved in the introjection of digital automata that may have been processed machine-to-machine by a number of computing systems before reaching a human 'consumer':

> Without such a politics, the inevitable destiny of the digital brain is to find itself slowly but surely short-circuited by *automata*, and thus find itself incapable of constituting a new form of society with other digital brains.

The question of personal data monetisation is part and parcel of such politics: can we develop a personal data ecosystem that allows for the trading of personal data in a way that is fair and comprehensible for individual human beings – or will the architecture we need to enable such trading take over and replace our individual discernment? This is not merely a question of trusted computing in the technical sense of having a secure environment with the right type of encryption to authenticate access and to guarantee the confidentiality of the content of our personal data. It is not even the question of the confidentiality, integrity and availability of my personal data. It is about the extent to which we can foresee what data derivatives we match and how this will constrain or enable us to develop our personal identity. Will personal data management, for instance, help to achieve such foreseeability? Will it re-enable a degree of autonomy or would it reinforce the heteronomy of individuals in the era of Big Data?

This raises another set of questions related to the nature of personal identity. Agre and Rotenberg have defined the right to privacy as:

> The freedom from unreasonable constraints on the construction of one's identity [16, p. 7].

This definition is more abstract, but maybe more effective that the more conventional definitions of privacy as (1) the right to be left alone and as (2) the right to decide when, how, and to what extent information about oneself is communicated to others. The first heralds the right to privacy as a liberty; a negative form of freedom, and the second heralds the right to privacy as the tool of a sovereign who reigns supreme over her personal data; a positive form of freedom. Both definitions have their drawbacks, and the beauty of Agre and Rotenberg's notion of privacy is that it acknowledges what is at stake with our privacy by referring to one's identity, while it also admits the relational character of privacy and the need to realise that constraints are, in principle, inevitable. Identity is relational, it is built while interacting with others and subject to all kinds of constraints. This is not a new fact, but perhaps the Enlightenment Age with its emphasis on the individual person has come to believe its own myth: that an individual person with an individual identity is an entirely independent and fully autonomous being that admits no interference from the outside. This is a line of thought investigated by the second Chapter in this volume, *Personal Data: Changing Selves, Changing Privacies*, by Charles Ess and Hallvard Fossheim. They explain:

> [T]he technologies of *literacy-print* correlate with high modern conceptions of the self as a primarily *individual self* – in Charles Taylor's terms, a 'punctual' or radically disengaged self (1989). Such an individual self, understood as a *rational autonomy*, and the modern liberal democratic state seem non-accidentally suited to each other.

They then suggest that:

> By contrast, both orality and secondary orality correlate with more relational conceptions of selfhood.

Secondary orality is a term derived from media studies, identifying certain characteristics in hyperlinked digital environments that compare to those of prehistoric, oral societies. One of these characteristics is a more relational understanding of self and a less unified notion of identity. They highlight the vulnerability of the relational self, and they warn that societies cherishing the relational character of the self tend to make the self dependent on social hierarchies, and seem to foster non-democratic politics. Though this is debatable, considering the egalitarian nature of many face-to-face societies [17], it seems clear that a relational self is more dependent on its environment than the unencumbered self of the Enlightenment's autonomous rational subject. This has major implications for privacy. According to Ess and Fossheim, societies that thrive on the idea of a relational self often have a negative opinion of privacy, as this is seen as an antisocial characteristic. They suggest that the current tendency to share and expose one's identity indicates a shift from atomistic notions of an independent self to more relational notions of an interdependent self. This, they argue, requires a new, hybrid understanding of the self as both relational and autonomous. This would require a shift towards, for instance, Nissenbaum's theory of contextual privacy [18]. The interesting question of how this relates to the monetisation and management of personal data within the context of the emerging personal data ecosystem remains unanswered, but in order to assess to what extent we can expect individual persons to effectively manage their personal data, we need to come to terms with the issue of individual autonomy and the impact of others, of technological infrastructures and of societal institutions on the self. Can we discuss personal data management in terms of individual consent and rational choice, or should we admit to the bounded rationality that forms the point of departure of behavioural economics? Is the rational liberal subject that forms the hidden premise of much talk over consent as autonomous as liberals proclaim, or should we admit the social nature of the self and thereby acknowledge the delicate mix of autonomy and heteronomy of individual persons? What does this mean for privacy: is it perhaps more than a private interest [19]?

4. Privacy as a Public Good

In this context, it is worth asking how the evolution of social norms, the development of technology and our normative, political and philosophical assumptions have interacted to create this particular example of the dialectic of Enlightenment. The answer might best be illustrated by considering the perhaps unexpected tension of personal choice and autonomy, as it is played out in the ideological and commercial arenas where the subtleties of political theory are so easily lost in the noise. So let us consider this dialectic in action.

Note that there is a health warning here: the arguments presented in this section are not normative ones, and this is not a piece of political philosophy. This section reports what happens when people with political, ideological, commercial and technological agendas conflict in a contested and ineffectively regulated space. The point here is not whether one believes that privacy, as related to autonomy and identity, is a precondition for a fair and free market, as well as for a viable democracy that requires individuals capable of making up their own mind. If you are reading this book, you probably subscribe to that complex proposition. In this section we consider how, and how not, to establish that point against those who do not believe it, those who believe it but think that care in this area is unnecessary, and those who believe that it is irrelevant to some of the current trends in technology which have caused concerns. Obviously, some would claim that the argument for privacy as a public good is a normative issue, and reformulating it in terms of a descriptive argument hides rather than removes normative assumptions. For the sake of the argument, we will, however, investigate the strength of a liberal position that is often invoked in favour of privacy as autonomy.

In a celebrated passage, political philosopher John Stuart Mill argued that:

> The sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant. He cannot rightfully be compelled to do or to forbear because it will be better for him to do so, because it will make him happier, because, in the opinion of others, to do so would be wise or even right [20, p. 14].

Let us call this the *Mill Test* of whether coercion (whether overt, or of the subtler 'nudge' kind) is justified to prevent harm (it is often referred to as the 'harm principle' [21]). It has become increasingly influential as freedom has become a prized political good, and now defines an area of private life where you have, in the classic account of Warren and Brandeis, the right to be let alone [22]. Ironically, the application of the Mill Test specifies a space for *decisional* privacy, but in our networked society decisions are often made to sacrifice *informational* privacy in exchange for free or useful services, even though many commentators believe that to do so is hardly wise or right at all. In less inflammatory terms, a decision is taken to exercise one's data protection rights which results in a loss of control over one's personal data – even if one retains rights of control under data protection law, these rights are seldom exercised and are, in practice, very hard to exercise.

When we apply the Mill Test to a decision to relinquish control over personal information – for example by joining a social networking site (SNS), and thereby colluding in the creation of a large amount of rich data about our social network and other aspects of our activities to the SNS owners – there is a tacit assumption made that the privacy that results from being invisible to the SNS benefits only the individual. Given that this is so, then in a 'civilized community' it is not acceptable to regulate SNSs by preventing or discouraging people from joining them in order to prevent them from carelessly giving their privacy away in a manner they might later regret. People can be informed of the potential for breaches of privacy, but if they continue to have a cavalier attitude towards their personal information that is their business. If privacy benefits the individual only, then it follows that lack of privacy may harm the individual only; the lack of potential for harm to others means that the Mill Test rules out any interference with the actions of individuals to preserve their privacy.

That analysis is shared by two usually antagonistic ideologies. Many liberals, libertarians and individualists champion the Mill Test, but privacy is important because it protects autonomy; the ability to make informed decisions in the absence of coercion. Without control over access to his person, reflections, decisions, and information about him, an individual is not fully informed about his environment, cannot be guaranteed to detect or avoid coercion and cannot be authentically himself [23].

Against that, so-called communitarians argue that freedoms only make sense against the background of a culture which maintains them. Rights entail responsibilities to ensure that communities function properly and humanely, and when individuals pursue their own rights beyond a certain point, the community suffers. Although they are important, privacy rights can undermine community cohesion, so when a community faces a well-documented threat (not just a theoretical one) to the common good, steps to curb privacy are not ruled out by the Mill Test. Etzioni lists a series of potential areas for intervention, including 'Megan's Law', a group of laws at both federal and state level in the US which require the addresses of convicted sex offenders to be publicly available [24].

Liberals and communitarians are generally in opposition, but in their joint support for the Mill Test, they agree implicitly that the gains of privacy accrue to the individual, while its costs are felt by wider society (perhaps in terms of loss of security, or lack of efficiency). Liberals and communitarians thus believe that privacy is a private good, like life, wealth and freedom. They think that unlike clean air, clean water and democracy, it is not a public good whose benefits accrue to the community at large.

This unusual consensus also finds support from those technological determinists who argue that the extent of privacy is a function of our deployment of information technology to undermine the so-called 'practical obscurity' which results from what Luciano Floridi has characterised as 'ontological friction' in information flow [25]. If technology makes it easier for information about an individual to get from A to B, and if that individual colludes with the deployment of that technology, then privacy is *de facto* difficult to protect, and some technological determinists – for example, Jeff Jarvis – argue that in that case it is socially harmful to do so [26].

Such determinism, rendered more plausible by the tacit assumption that the technology itself plays only a neutral role in this novel scenario, was famously expressed by Scott McNealy as "you have zero privacy anyway. Get over it." Facebook CEO Mark Zuckerberg has also often argued that the reduction of privacy in the Web-enabled world is solely a result of the unforced take-up of privacy-inhibiting technologies changing social norms.[10]

These arguments bring with them the unspoken implication that the technology has no effect on social norms, and users take up privacy-threatening technologies that are already and independently acceptable to them. This argument, which tends to come from technology companies and cyber-enthusiasts, is surely disingenuous, if not self-serving.

Rather, we find ourselves facing a new paradigm. When surveillance, data production and data analysis were the prerogatives of governments and large corporations, individuals gained little from visibility – privacy was the right to be left alone. Data tended to be created in separate and extra processes – for example, data about shopping

[10] In honour of Zuckerberg's role in crafting this deterministic position, one author of this introduction has christened it 'Zuckerbollocks' [27]. We should make it clear that Zuckerbollocks is a populist rendering of technological determinism, rather than a carefully thought-out and philosophically-respectable position, and when we talk of technological determinism in this section we specifically refer to Zuckerbollocks.

habits was gleaned by market research companies asking people to fill in questionnaires. Filling in forms was tedious, and there was little incentive for consumers or citizens to cooperate by doing so. Demand for data exceeded supply. Now, digital transactions increase the supply of data by producing data as an organic by-product of an online transaction. A person looks at a web page, buys a book, uploads a photo, sends a text – the observed data recording the transaction is created naturally and immediately. The massive supply of data has laid the groundwork for the design and production of innovative services (which themselves generate even more data), and which not only provide value for companies and governments, but allegedly also the data subjects. Moore's Law means that processing power has kept pace with this increase in data supply.

So for the first time we find ourselves in a world where there are many enticing incentives for consumers and citizens to risk their privacy by exercising their data protection rights, and becoming visible to their networks. If we take a revealed preference view of belief-desire psychology, individuals' behaviour in this new world shows that they (or many of them) prefer the benefits of visibility to the now rather old fashioned idea of being private. They assess its benefits and costs, and make a decision accordingly. This may not be easy – how do you compare the immediate benefits of providing data about oneself with the theoretical risk, several years down the line, of its being misused? – but that is no different in principle from many similar discounting decisions we make in the ordinary course of events. The benefits can be quantified – in 2010, the value of free services funded by surveillance-based advertising, minus a discount for foregone privacy, was estimated at over €100 billion [28].

Liberal arguments about the value of privacy in its protection of autonomy [23] now seem theoretical and unrealistic as more people flock to SNSs and see benefit in playing with identities and self-descriptions, and exploring new types of meaningful interaction. Most people are reasonably clear about the artificialities of SNSs (e.g. they know the difference between a real-world friend and a Facebook friend), and are prepared to experiment – few are completely passive consumers [29]. Loss of autonomy may be compensated for by increased control over identity and self-presentation. To many, the ability to play with identity is a real and present benefit, and the loss of autonomy a complex, theoretical and distant postulate of political philosophy.

So the liberal, by assuming the application of the Mill Test to decisions about data, cedes so much ground to the technological determinists that it becomes difficult in the extreme to defend privacy.[11] The liberal arguments to defend privacy tend to point to theoretical harms to society as a whole. For example, [30] argues cogently that privacy is essential to the basic values of the European tradition – self-determination, democratic participation and economic well-being. But these philosophical and normative arguments are not guaranteed to be accepted by opponents who constantly make the demand: *show me another individual who has been harmed tangibly by my actions in consenting to allow third party access to my data*.

Although privacy is immensely important to a liberal society, classical liberalism will undermine itself if it cannot accede to this demand. Is there a way out of the impasse?

[11] This isn't quite true. There are arguments available that an individual's autonomy has a social value as well as value to the individual (for example, it enables democracy to function more effectively). However, these arguments tend to rest on liberal assumptions, and so do not always appeal widely to non-liberals, and are not effective to *defend* liberalism against hostile attack.

Fortunately, there is. Arguments that can meet the demands of the opponent are readily available, although not made as often as they should be.[12]

- **Accountability.** An individual's autonomy has a social function – only autonomous persons are properly accountable. When a person's privacy is diminished, the question about his responsibility for his actions becomes muddied – and the loser is wider society, not that person himself [19,31].
- **Profiling.** Many decisions are framed by the use of data to classify people and 'personalise' (or, put another way, 'restrict') choices. When others forego privacy, their data can create a stereotype against which a privacy-sensitive individual may be matched despite her attempts to maintain control [10,32,33]. The stereotypes can be developed from group behaviours, and need not include anything about the individual herself, except to place her in the group (perhaps for demographic reasons – she is a divorced executive aged 41–50 – or because she lives in a particular postcode or zip code area).
- **Security.** Much writing on privacy assumes a security/privacy trade off. Privacy is a right, but security is a primary function of the state. Yet even if this trade off sometimes exists, is it the usual condition? Arguably not – a loss of privacy can result immediately in a loss of security when data become public, or are leaked [34,35].
- **Trading data.** Because data is economically valuable, there is a case for commodification to allow the data subject to profit alongside data processors [36]. Yet without the measure of control that privacy brings, asymmetries of knowledge would make the functioning of such a market inefficient [37]. Could citizens meaningfully consent to their data being exploited without any idea of how and in what context it will be used?
- **Credible signalling and full disclosure.** New markets are being created as increased data lowers the costs of credible signalling. For instance, a social network is a good indicator of creditworthiness, so an individual could agree to make their SNS data available to a lender in return for a discounted interest rate.[13] This may help the underbanked and those without collateral. However, there is a danger that those who do not wish to disclose data will be penalised on the assumption that their data would not provide a positive signal; in the banking example, a privacy-aware individual would automatically be assumed to be uncreditworthy [38].
- **Chilling effects.** As privacy decreases, behaviour will adapt. Even in the absence of overt censorship, people will experiment and innovate less, and express themselves less freely [9]. This may be a particular effect of the recent revelations about PRISM.

These various arguments all demonstrate the importance of privacy as a public or social good without relying on liberal premises. If any of these arguments is convincing, then it follows that the Mill Test does not apply to privacy, and that society may take steps to protect privacy even in the face of mass market behaviour which reveals preferences for other goods over privacy.

[12] This argument is made in more detail in [27].

[13] Examples of companies that are exploring this business opportunity include Kreditech (http://www.kreditech.com/), Neo (https://www.myneoloan.com/) and Lenddo (https://www.lenddo.com/).

In fact we may go further. They basically confirm that liberal notions of purely autonomous individuals, communitarian celebration of collective identity and technological determinism all miss the point. Individuals are always relational; they emerge from the various communities in which they participate and they also co-constitute these communities. Information and communication technologies mediate the process of identity construction, but do not over-determine either individual or society. These arguments build on a more robust understanding of self, technology and society, acknowledging the inherently relational character of privacy.

For the user-centric data management systems considered by the chapters in this book, then, there are indeed important reasons why privacy protection needs to be built into the architectures and system designs. Personal data management should not simply endow the data subject with the ability to sell to the highest bidder. Many of the chapters in this book discuss regulations, architectures and technologies which will begin to help us negotiate the tricky line between maximising the value of our data and minimising our exposure to unwelcome surveillance, and to help us draw lines (either in law or via social norms) when immediate personal gain threatens to produce long-term social loss.

5. Overview of the Chapters

Such is the political, legal and technical background in which we find ourselves in 2013. We are grasping to find solutions to problems we perhaps only dimly perceive – or worse, we are looking for problems which may not exist while missing the serious issues just around the corner. We do not know whether solutions should be given the full power of law, or whether a quick techie fix will do the trick. Meanwhile, the market presents its own dialectic and generates the solutions for which people will pay. Is the market excluding large sectors of the population, and will the discourses it produces warp or invade public space? And are innovation and social norms in any event moving so quickly that it is futile for institutions to try to keep up?

The Digital Enlightenment Yearbook 2013 has collected a series of chapters exploring the idea of the value of personal data. The different stakeholders in society and the different scientific communities (technology, law, philosophy, social science, economics), as well as entrepreneurs and policymakers, will have very different opinions and perspectives on this motive. Our intention in this book was to bring together these different perspectives to form a basis for inspiring and constructive discussions across disciplines. Most were written especially for this volume, but a small minority are reworkings or repurposings of previously published material.

We are also extremely grateful for a Foreword by Robert Madelin, and an Afterword by Kim Cameron. Both of these pieces place our thinking into the wider context of big data, its promise (Madelin) and its dangers (Cameron). How, the reader may think, is the poor individual to cope, tossed about in the tsunami of data, services and innovation that is engulfing her? Both Madelin and Cameron agree that PDM is an essential part of the story, and the papers in this collection go some way to filling in the detail.

5.1. Part I: Background

The chapters are divided roughly into five main groups – of course in a volume of this nature there is a lot of inter-group overlap and intra-group heterogeneity, which is a roundabout way of saying that the editors (themselves a diverse trio) had some trouble deciding which chapters should go where. Part I provides a background, and continues with some of the themes discussed in this introduction. The two chapters in this section, by Stiegler, and Ess and Fossheim, have been discussed at length above. They set the scene for the more detailed examination of the concepts of personal data management and valuation in the remaining chapters. Following this opening section, four more follow.

5.2. Part II: The Need for Privacy

Part II moves from the general issues surrounding our new digital world, to the more particular considerations and challenges of the problem of personal data and its use and abuse, its protection and commoditisation. Sociology, psychology and policy are all explored here as we consider the ways in which the individual responds to and is shaped by technology. The individual wishes to determine her own identity – how can she use her own data to do that, and how can she control the process? Put another way: how do informational self-determination and privacy interlink so that each needs the other?

Lizzie Coles-Kemp and Joseph Reddington's chapter, entitled *Not So Liminal Now: The Importance of Designing Privacy Features Across a Spectrum of Use*, pushes beyond the mainstream of computer use to examine how the glut of personal data being created will affect sectors of society that are often neglected by technology markets and data regulators. Assumptions are made about data subjects' cognitive abilities that are simply unrealistic in the general case, and much of the discussion of how the new environment affects the autonomy of individuals is predicated on the possibility of them refusing to use a technology. Coles-Kemp and Reddington argue that neither of these optimistic assertions is necessarily true. They take a specific example – that of people with severe speech defects who use Augmentive and Alternative Communication systems (AAC) – in which complex problems of data storage and data use crop up that perhaps would not have been anticipated. Yet the solutions proposed by AAC developers do perhaps contain lessons for more widely available and applicable technologies.

In their chapter on *Privacy Value Network Analysis*, Adam Joinson and David Houghton address the notion of privacy value head on. They use methods from network analysis and the social capital literature to analyse and visualise the creation of value across a network. As we have noted above, there is real value for consumers created by networks, and any privacy-aware individual needs to make highly complex calculations as to how much information she can release – and even then there is an important question as to how informed she can possibly be about its use (a lacuna that a number of papers in this volume attempt to fill). Consumers generally can be disturbed when specific advertising practices are made clear to them (Google's Eric Schmidt once famously described his own company's policy as being "to get right up to the creepy line" – a notion that is in itself so creepy that it raises creepiness to the metalevel). Joinson and Houghton overlay techniques from value network analysis with ideas about managing communications at the boundary of our selves, our personal relationships and our group memberships to visualise notions of information exchange, the goals of interaction and the impacts across the network. In this way they hope to express, and ultimately to influence, decisions made to disclose or not disclose information.

Ann Cavoukian's chapter, *The Personal Data Ecosystem (PDE): A Privacy By Design Approach to the Pursuit of Radical Control*, describes the technological components of the evolving idea of a personal data ecosystem (PDE – defined earlier in this introduction). Cavoukian takes the idea of privacy by design (PbD) seriously – this is the notion that, when designing systems that will hold or otherwise deal with personal data, one should design it with the privacy of the data subjects as a first order feature of the system, as opposed to the all too common practice of designing a system that does everything the business model demands, and then tacking a privacy management component onto the design as an afterthought. PbD, one would think, is an obvious way forward, yet it is proving strangely (or not so strangely!) difficult to promote. Cavoukian describes the ideal of 'radical control' over our personal data , which she argues should underlie the design of any PDE. In the absence of trust in government to resist pressure from large commercial players and from its own intelligence communities, radical control may well be the only way forward to protect individuals' data unconditionally. Put another way, if we wish to inject privacy by design into PDEs, Cavoukian argues that it is essential to put control totally in the hands of the individual; if it is contracted out to governmental actors, we are lost. It is certainly interesting, when considered in the context of the rest of the chapters in this book, that many of the components of radical control are addressed separately, which is suggestive of the grand sweep of the ambition of this chapter. But Cavoukian appears to argue that without such ambition, privacy cannot be protected in full.

Alexander Novotny and Sarah Spiekermann's chapter signals equal ambition, in its title: *Personal Information Markets AND Privacy: A New Model to Solve the Controversy*. In company with many other chapters, Novotny and Spiekermann start from the extraordinary business value derived from personal data, and consider the loss of trust that consumers feel as their data is swapped, shared and analysed outside any apparent control. The control that is afforded, for example, by Privacy Enhancing Technologies, requires more input than the poor consumer is prepared to put into the matter. Life is not only not private, but it is too short to make it private. Novotny and Spiekermann propose a three-tier model for markets in personal data and information, in which money can be made but privacy also protected. The first tier contains the data subjects and those organisations with which they have a direct relationship. The second tier contains the business service providers which support the first tier operations. The third tier is everyone else in the market who cannot deal direct with personal data. Breaking markets down like this, the model is able to specify a set of rights and responsibilities for each actor, and technological and legal enablers for each relationship, many of which already exist in current regulation but which may not always be properly enforced. The authors recognise several challenges to their model, some technical – for example, the need to ensure anonymisation of data when it reaches the third tier – and others more practical, including global enforcement. Nevertheless, the model disaggregates a number of intertwined norms and drivers in information markets, and enables us to think somewhat more clearly about how such markets could be designed to benefit everyone.

5.3. Part III: Architectures for PDMs and PDEs

Part III brings together papers which describe potential architectures at a relatively high level of abstraction. Here, we look not at proposed systems but at types of technology, considering what issues they raise and what problems can be solved when we consider the functional units within systems and the relations between them. What are the properties that systems will need in order to foster privacy or to support flexible, informed consent?

Online Privacy: Towards Informational Self-Determination on the Net, the chapter by Simone Fischer-Hübner et al. decries the current status of online privacy provision and the way in which we have sleepwalked into a world where privacy is routinely compromised in order to fund free services such as search and social networking support. Informational self-determination appears to have been lost in the rush to exploit and monetise personal data. The chapter, an updated version of a manifesto written and published in 2011, reviews the state of the art in privacy provision, and argues that current PETs lag behind the progress made in unlocking the meaning in data, and often fall down on important characteristics such as usability and scalability. No wonder demand appears to be low. They identify a series of challenges, including introducing transparency about the use of data and the risks to privacy, and the provision of workable tools. Their third challenge is identity management systems that undo information asymmetries and restore control of identifying information to the individual, and this may well be a crucial and neglected part of the picture. Their ten recommendations for regulatory change, and four recommendations for further research, set out a manifesto which puts the individual at the centre of data management.

Johannes Buchmann et al. focus on online social networks in their chapter *Personal Information Dashboard: Putting the Individual Back in Control.* The self-explanatory title indicates their approach of providing intuitive visualisations and automatic tools for bringing together data from a range of sources to allow the user to understand the nature of the footprint she makes across the range of her online identities – a step toward the transparency which is called for by Fischer-Hübner et al. Techniques such as machine learning and correlation models allow the presentation of options for lowering privacy risk (assuming that is what the individual wants). If she does not, then at least she is informed about the risks to privacy that she runs. Buchmann et al. set out in detail an architecture including a series of privacy-enhancing features and components to calculate current levels of privacy and to aid in decisions about what to make public.

Uninformed or unconditional consent is a problem identified by both Fischer-Hübner et al. and Buchmann et al. Edgar Whitley contributes a study of technical methods for supporting informed consent in his chapter *Towards Effective Consent-Based Control of Personal Data*. Consent is a cornerstone of existing data protection, although as Whitley shows, current information systems tend to treat it as a simple concept, a black box that either allows or disallows the processing of data. However, as a matter of fact, our views of how our data should be accessed and used are likely to be more nuanced in a real-world context. Furthermore, consent needs to be informed, yet – as a number of papers in this collection make clear throughout – it is far from established that a typical data subject is genuinely informed about what goes on, given the quantity of data floating around cyberspace and the sheer complexity of the various transactions in which it is central. Indeed, many institutions engineer their interactions with data subjects so that consent decisions are skewed, creating the illusion of informed consent. Does too much hang on the concept of consent, then? Whitley explores the possibility of a more dynamic and user-centred notion of consent supported by technology, but informed by wider social science research.

5.4. Part IV: Other Sources of Data

Part IV is a digression which connects with our main theme through the use of data. We have focused, in this introduction, on data about an individual, whether volunteered, observed or inferred. In managing her own data, the individual is in general likely to be using data she herself has generated, yet this is dwarfed in quantity by data held by others (banks, supermarkets, energy companies). Add to this the extra data to which she arguably has a right (government data), which is relevant to her, if not directly about her (data about her local community, schools, roads, transport timetables), and suddenly her PDE looks very rich and valuable to her personally – *if* she can get hold of that data and use it effectively.

The push toward open data, which has developed enormous momentum in a very short space of time [39], creates another source of valuable data about the communities in which the individual lives and works. Open data, machine readable and online under highly liberal licences, can be exploited for any purpose, and it is hoped will revolutionise government and commerce. New innovative services will be built on the back of open data stores, and will be part of the big data story that Robert Madelin's Foreword looks forward to. However, open data, with the consequent lack of control that this implies, brings its own issues to the individual as well. No government would publish personal data as open data, but how about open data derived from personal data (aggregated or anonymised)? How about open microdata? The law here is somewhat untested, and two papers explore the interesting nexus between open data and personal data from a legal perspective. A third looks at the provision of data about individuals *to* those individuals by business.

Ugo Pagallo and Eleonora Bassi, in their chapter *Open Data Protection: Challenges, Perspectives and Tools for the Reuse of Public Sector Information*, consider the relation between personal data and open data, considering the large amount of public sector information (PSI) which is derived from personal data, such as registrations of vehicles or land. They stress the real possibility of a "divorce" between rights to data and data protection, then explore the role of privacy by design as a marriage guidance counsellor might. There are several mechanisms, including privacy impact assessments and anonymisation techniques, which individually may not be sufficient to prevent a split, but which in aggregate may allow progress; they also would wish to include the notions of control and sensitivity to user preference that several authors have already advocated. They argue that, in the right regulatory and technical context, privacy and openness are not in a zero sum game.

Katleen Janssen and Sara Hugelier's chapter *Open Data: a New Battle in an Old War Between Access and Privacy* examines the same question from a more historical perspective, looking at how law has developed to help us balance rights to information with the rights to control, suppress or filter information which seem to constitute the positive privacy right. The drivers for freedom of information and open data seem very different – FoI mechanisms are generally seen as a kind of redress or remedy following a reasonable request for information that has been denied, while open data is a positive decision to release data. One does detect arguments about rights to data within the open data movement, but, in general, innovation and growth seem to be the main political drivers. Indeed, rights to privacy appear to be much more fully developed in law than rights to information. Janssen and Hugelier revisit older law resolving conflicts between transparency and privacy to gain insights into the potential for conflict in a world of open data.

Sir Nigel Shadbolt reviews the UK government's midata initiative, working with the private sector to give data subjects access to the data that has been collected about them, in his chapter *Midata: Towards a Personal Data Revolution* – a title which shows the level of ambition for this programme. Data protection law guarantees an individual access to the information about her, but midata aims to make that routine. As with open data – a programme with which midata has much in common – there is no specific target to aim at. Midata is intended to stimulate new markets, and it is envisaged that individuals could gain a lot of value simply by visualising and then adapting their own consumption patterns. Several case studies are described, such as energy use, which in the era of smart grids, high energy costs and concern about the environment looks like a potential winner. The legal context of midata is complex, and Shadbolt describes the different approaches of the UK, the EU and the US. The midata initiative, like open data, provides another piece of the PDM jigsaw – we need technology to manage our data, but how much more powerful that model will be if we can secure access to some of the extremely rich data about us and our environment held by other organisations.

5.5. Part V: Personal Data Management: Examples and Overview

It is surprising how often a book on technology policy makes assumptions and lays down the law in an abstract way, independent of actual developments. Equally, it is also often the case that a particular form of technology is taken by commentators to be the paradigm for future developments, only for both it and the commentaries to be made obsolete by next year's wonder. It is of course hard to make a book on technology future-proof, but we hope that the debates within these covers will resonate beyond the situation at the time of writing in the summer of 2013.

To that end, we invited a number of key players in the field of user-centric personal data management to write chapters describing their views of the field, how we have got to where we are, and where we might go in the future. In particular, we asked these authors to set out what systems, methods, tools or formalisms they had implemented to help answer the reader's obvious question: what is out there *now*? Of course at the time of writing we cannot know the future, but we have sampled the present, and in future years readers will be able to consider how far such systems have been influential. For now, these chapters provide a level of context which allows the reader to understand some of the sometimes very abstract discussions which occur throughout the book, and to get a sense that the politics of this area are very much current.

Carolyn Nguyen et al. look at the collection of information by businesses in their chapter *A User-Centered Approach to the Data Dilemma: Context, Architecture and Policy*. They point out the dilemma that regulation to protect the individual may threaten the free flow of information, dampening innovation and undermining companies' business models, and argue that the way round this dilemma is itself technological. They describe an architecture to handle metadata which will associate user preferences and permission with data, allowing users the flexibility to change their policies and consider unanticipated uses of their data. The core of their chapter is empirical work carried out by Microsoft (the affiliation of the authors) to understand user attitudes toward personal data, identity and trust – this is particularly welcome, as there is a surprising lack of such empirical work being used directly in system design or, as in this chapter, the principles that form the framework for fair use of data. The metadata architecture is intended to allow data to flow, but with the privacy policies of the data subjects alongside it, with the aim of circumventing the 'data dilemma' described earlier.

Martin Kuppinger and Dave Hearns describe their vision for Life Management Platforms (LMPs), whose purpose is clearly signalled in the subtitle of their chapter (adapted from a previously published report) *Control and Privacy for Personal Data*. An LMP is a means of consolidating data from various sources, especially sensitive data, and Kuppinger and Hearns argue that we can go beyond current notions of personal data stores in terms of the flexibility of support for security and privacy. A 'personal domain' of data is the metaphor in which ideas of minimal disclosure and retention of control are explored. The authors set out their business model which, if feasible, promises to open up an interesting space for solutions to appear, although they remain aware that there are still many inhibitors which could suppress the sector.

William Heath et al. have a similar agenda, described in their chapter *Digital Enlightenment, Mydex and Restoring Control Over Personal Data to the Individual*, in which they describe the Mydex system in the context of an idiosyncratic but undeniably recognisable history of the drivers of the erosion of privacy by technology. Like Kuppinger and Hearns, Heath et al. are keen to establish the possibility of a feasible business model for personal data management systems, in their case based on a 'Catherine wheel' model (a type of firework where a series of separate, simultaneous ignitions drive the firework round) where benefits are seen for the individual and the organisation, as well as contributing to the economy of volunteered personal information. Mydex is a social enterprise in the UK which aims to develop tools to help people realise the value of their personal data online while also supporting informational self-determination, and Heath et al. describe their own system, while welcoming the growth of a vibrant sector in which there are many players and many alternatives. They describe the architecture and design of Mydex, both in functional terms but also with a historical perspective, showing how their community prototype led to particular issues and drove particular solutions. The historical, almost Hegelian, perspective of this chapter gives a strong sense of how hard it will be to provide a futureproof roadmap for the development of personal data ecosystems.

To conclude this section, Jacques Bus and Carolyn Nguyen consider the state-of-the-art range of practical examples in the field (including examples from other chapters in this book), and in their chapter, *Personal Data Management – A Structured Discussion*, they abstract away from the complexities to produce a framework for considering how to frame the debates about the use of personal data. Many basic terms are defined, including – as noted above – personal data management, and a reference model for representing the requirements of context-based PDM, which requires the basic infrastructure, the elements which allow management of data, and the elements that allow interaction between the user and external parties. From this reference model, Bus and Nguyen work to create a framework which proposes a set of relations in which trust can be negotiated and placed accurately and rationally. The proposal is intended to support and promote dialogue and discussion without necessarily presupposing particular solutions or market structures. Nevertheless, even the creation and support of such a trust network would already be a long way along the road from the current state of exploitation and ignorance to the radical control of Cavoukian, or the defined and enforced rights of Novotny and Spiekermann.

6. Research Agenda

It may seem that we fully endorse the idea of user-centric Personal Data Management, even though this does not imply that we would necessarily endorse user-centric Personal Data *Monetisation*. At this point in time, however, the editors do not agree on whether PDM will enlighten us. There are worries about the further 'datafication' [9, p. 73 ff.] of personal identity, increasing discretisation and commodification of invaluable and untradeable dimensions of human agency and concerns about slipping from PDM as 'management' to PDM as 'monetization'. What we do endorse, however, is further research into the potential of PDM for user empowerment. That PDM will achieve the redressing of power imbalances between the 'owners' of Big Data and the individuals they apply to cannot be taken for granted, and such research should also raise the question of what problems cannot be solved by means of data management and what problems may be created or reinforced by developing tools and frameworks to manage one's data. So we end with a cross-disciplinary research agenda of three pivotal questions:

1. What problems can current models of PDM solve?
2. What problems cannot be solved by PDM systems?
3. What new problems might be created by effective employment of PDMs?

This is not the place to answer these questions, precisely because this will require both empirical investigation and philosophical reflection. As to the first question, we need to investigate the difference and similarities between identity management and personal data management and the extent to which PDM facilitates access to and/or usage of personal data. Does PDM provide possibilities of profile transparency, enabling users to foresee how advertisers, law enforcement, potential employers, credit providers and insurance companies will 'rate' them? As to the second question, as in the case of identity management, it is important to flesh out whether PDM helps in ensuring purpose specification and purpose limitation, and whether it provides intuitive transparency regarding third party access and usage. How does PDM relate to the novel rights of data portability and the right to be forgotten? Can PDM help in providing control over observed and inferred data or is this an illusion in the era of Big Data? If so, what does this mean in an age where algorithms increasingly inform a host of decision systems that run on observed and inferred data and hardly require volunteered data? Does PDM protect against the application of inferred profiles that have been derived from anonymised and/or aggregated data, or does this fall outside its scope? As to the third question, to what extent does PDM require root identities that are 'real identities', thus incentivising increased use of real identities to gain access to all kinds of services that are now easily accessible by means of fake identities? Does PDM ignore the maxim that trust does not scale; would it make us dependent on trust frameworks and vulnerable to the volatility of high frequency trading with personal data? Might PDM turn our indeterminate personal identity into something that can be measured and mined, thus inviting us to participate in the process of monetisation of our behaviour?

The only correct answer will be: 'it depends'. On how we engineer, design and negotiate existing and emerging personal data ecosystems and on how we integrate them into our life world. How we arrange for countervailing powers between Big Data 'owners' and individual persons. The idea of countervailing powers is another Enlightenment idea, going back to Montesquieu. This volume is a call to scrutinise the various types of PDM that are proposed, to develop new ways to empower individual persons and to reinvent the checks and balances of constitutional democracy in the face of novel knowledge asymmetries.

Acknowledgements

During the editing of this book and the writing of this Introduction, KOH was supported by SOCIAM: The Theory and Practice of Social Machines, funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/J017728/1, and MW was supported by the European Center for Security and Privacy by Design (BMBF) and the Center for Advanced Security Research Darmstadt (LOEWE). Our thanks to the many scholars and professionals who peer reviewed the chapters for us.

Thanks also to Rob Cottingham for supplying the illustration on page 1, reproduced here under Creative Commons Non-Commercial Attribution License.

References

[1] G. Bateson, *Steps to an Ecology of Mind*, Ballantine, New York, 1972.

[2] T.W. Adorno & M. Horkheimer, *Dialectic of Enlightenment*, Herder & Herder, New York, 1972.

[3] J. Gray, *Enlightenment's Wake: Politics and Culture at the Close of the Modern Age*, Routledge, London, 1995.

[4] J. Palfrey & U. Gasser, *Born Digital: Understanding the First Generation of Digital Natives*, Basic Books, New York, 2008.

[5] K. Schwab, A. Marcus, J.R. Oyola, W. Hoffman & M. Luzi, *Personal Data: The Emergence of a New Asset Class*, World Economic Forum, 2011.

[6] M. Hildebrandt and K. de Vries, (eds.), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, Abingdon, 2013.

[7] E. Goffman, *The Presentation of Self in Everyday Life*, Anchor Books, New York, 1959.

[8] M. Dodge & R. Kitchin, 'Outlines of a World Coming Into Existence': Pervasive Computing and the Ethics of Forgetting, *Environment and Planning B: Planning and Design*, **34** (2007), 431–445.

[9] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton, 2009.

[10] M. Hildebrandt, The Dawn of a Critical Transparency Right for the Profiling Era, in: J. Bus, M. Crompton, M. Hildebrandt & G. Metakides (eds.), *Digital Enlightenment Yearbook 2012*, IOS Press, Amsterdam, 2012, 41–56.

[11] A.L. Allen, Dredging Up the Past: Lifelogging, Memory and Surveillance, *University of Chicago Law Review*, **75** (2008), 47–74.

[12] N. Watt, PRISM: Claims of GCHQ Circumventing Law Are 'Fanciful Nonsense', Says Hague, *The Observer*, 9th June, 2013, http://www.guardian.co.uk/world/2013/jun/09/prism-gchq-william-hague-statement.

[13] J. Borger, L. Harding, M. Elder & D. Smith, G20 Summit: Russia and Turkey React with Fury to Spying Allegations, *The Guardian*, 17th June, 2013, http://www.guardian.co.uk/world/2013/jun/17/turkey-russia-g20-spying-gchq.

[14] E. MacAskill, J. Borger, N. Hopkins, N. Davies & J. Ball, GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications, *The Guardian*, 21st June, 2013, http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[15] M. Wolf, *Proust and the Squid: The Story and Science of the Reading Brain*, Icon Books Ltd, Thriplow, 2008.

[16] P.E. Agre, Introduction, in: P.E. Agre & M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, MIT Press, Cambridge, Massachusetts, 2001.

[17] M. Sahlins, Poor Man, Rich Man, Big Man, Chief: Political Types in Melanesia and Polynesia, *Comp. Stud. Soc. Hist.*, **5** (1963), 285–303.

[18] H.F. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford, Calif., 2010.

[19] M. Hildebrandt, Privacy and Identity, in: E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp, 2006, 43–58.

[20] J.S. Mill, On Liberty, in: *On Liberty and Other Essays*, Oxford University Press, Oxford, 1991, 1–128.

[21] J. Feinberg, *The Moral Limits of the Criminal Law Vol. 1*, Oxford University Press, New York, 1987.

[22] S.D. Warren & L.D. Brandeis, The Right to Privacy, *Harvard Law Review*, **4** (1890), 193–220.

[23] B. Rössler, *The Value of Privacy*, Polity Press, Cambridge, 2005.

[24] A. Etzioni, *The Limits of Privacy*, Basic Books, New York, 1999.

[25] L. Floridi, The Ontological Interpretation of Informational Privacy, *Ethics and Information Technology*, **7** (2005), 185–200.

[26] J. Jarvis, *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*, Simon & Schuster, New York, 2011.

[27] K. O'Hara, Are We Getting Privacy the Wrong Way Round? *IEEE Internet Computing*, **17** (2013).

[28] IAB Europe, *Consumers Driving the Digital Uptake: The Economic Value of Online Advertising-Based Services for Consumers*, White Paper, 2010, http://www.iabeurope.eu/media/95855/white_paper_consumers_driving_the_digital_uptake.pdf.

[29] N.B. Ellison & D.M. Boyd, Sociality Through Social Network Sites, in: W.H. Dutton (ed.), *The Oxford Handbook of Internet Studies*, Oxford University Press, Oxford, 2013, 151–172.

[30] acatech, *Internet Privacy: Taking Opportunities, Assessing Risks, Building Trust*, National Academy of Science and Engineering, Munich, 2013, http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_Internet_Privacy_Pos_eng_final.pdf.

[31] C. Sunstein, *Republic.com*, Princeton University Press, Princeton, 2001.

[32] T.Z. Zarsky, 'Mine Your Own Business!': Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion, *Yale J. Law Technol.*, **5** (2003), 17–47.

[33] M. Hildebrandt & S. Gutwirth, *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008.

[34] J. Waldron, Security and Liberty: The Image of Balance, *J. Polit. Philos.*, **11** (2003), 191–210.

[35] M. Hildebrandt, Balance or Trade-off? Online Security Technologies and Fundamental Rights, *Philos. Technol.*, doi:10.1007/s13347-013-0104-0 (May 2013).

[36] L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

[37] P.M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control and Fair Information Practices, *Wis. Law Rev.*, (2000), 743–788.

[38] S.R. Peppet, Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future, *Northwestern University Law Review*, **105** (2011).

[39] N. Shadbolt & K. O'Hara, Linked Open Government Data, *IEEE Internet Computing*, **17** (2013).