Article

European Journal of Social Theory
2017, Vol. 20(3) 329–347

DOI: 10.1177/1368431016679167
journals.sagepub.com/home/est

Digital, politics, and algorithms: Governing digital data through the lens of data protection

Rocco Bellanova
Peace Research Institute Oslo, Oslo, Norway; Université Saint-Louis – Bruxelles, Brussels, Belgium

Abstract
Many actors mobilize the cognitive, legal and technical tool-box of data protection when they discuss and address controversial issues such as digital mass surveillance. Yet, critical approaches to the digital only barely explore the politics of data protection in relation to data-driven governance. Building on governmentality studies and Actor-Network-Theory, this article analyses the potential and limits of using data protection to critique the 'digital age'. Using the conceptual tool of *dispositifs*, it sketches an analytics of data protection and the emergence of its configuration as 'data protection by design and by default'. This exploration reminds us that *governing through data* implies, first and foremost, *governing digital data*.

Keywords
algorithms, data protection, digital, digital data, governmentality, politics

Privacy may be dead, but data protection is alive and kicking. In April 2016, the European Parliament and the European Council adopted a new comprehensive data protection framework (European Parliament and Council, 2016a; European Parliament and Council, 2016b), bringing to a tentative closure the long and complex policy-making process and its implications for individuals, states and corporations (EP Press Service, 2016). Even outside the European Union (EU) institutional arena, many socio-political

Corresponding author:
Rocco Bellanova, Peace Research Institute Oslo (PRIO), Hausmanns gate 3, 0186 Oslo, Norway.
Email: rocco@prio.no

actors – ranging from civil liberties advocates to IT companies and regulators – use the cognitive, legal and technical tool-box of data protection when they discuss and tackle controversial issues, such as digital mass surveillance (Bennett, 2008; Regan, 2012). The data protection solutions they propose are often very different from each other, if not conflictive, so that it is impossible to define unambiguously what data protection is and what it does (Raab, 1997; Rouvroy and Poullet, 2009; Gutwirth et al., 2010).

This article analyses the potential and the limitations of using data protection to critique the politics of the 'digital age', where digitized information, computing systems and cybernetics have become cornerstones of the practice and the conceptualization of contemporary governance (Hood and Margetts, 2007; Pasquale, 2015; Supiot, 2015). Indeed, whenever data protection is mobilized by actors, what seems to be at stake is the question of 'how not to be algorithmically governed *like that*' (rephrasing Foucault, 2003b: 265, italics in original). In other words, data protection participates in an internal critique about the least intrusive and yet more productive forms of data-driven governance. For instance, a central theme of the data protection reform has been the two-fold ambition, first, to ensure that people could 'regain control of their data', and, second, to design solutions that favour the exploitation of the economic and social potential of digital technologies (EP Press Service, 2016). In some cases, as shown in the analysis below, data protection is shaped into specific socio-legal and technical devices that contribute to foreclosing the space of disagreement within data-driven governance. Yet, if anything is proper to data protection, it is not a supposed sheltering power, but rather, the obduracy of the ripples that it leaves when it participates in the folding of data, people, software, institutions, hardware, etc. into a given politics of the digital.

This contribution builds mainly on governmentality studies (Dean, 1999; Miller and Rose, 2008; Rose, 2004 [1999]; Rose and Miller, 1992; Walters, 2012), in particular where they meet with Actor-Network-Theory (Akrich et al., 2006; Latour, 2005; Law and Hassard, 1999). Neither of these literatures offers a rigid and ready-made theoretical framework to study data-driven governance. However, they are highly relevant insofar as they point to the epistemic and political advantages of investigating governance as 'an eminently practical activity' (Walters, 2012: 2), where power circulates and can be exercised through the design, use and contestation of manifold devices (Latour, 1986), from quantification mechanisms to record-keeping and high-tech security systems (Amicelle et al., 2015). In a similar vein, an increasing number of scholars from (critical) security and surveillance studies (Amoore and de Goede, 2012; Andrejevic and Gates, 2014; Introna and Wood, 2004; Leese, 2014; Lyon, 2014) and from media and software studies (boyd and Crawford, 2012; Cardon, 2015; Chun, 2011; Gillespie, 2014; Kitchin and Dodge, 2011; Ziewitz, 2016) highlight the need to understand governance by focusing on *algorithms*, i.e. 'encoded procedures for transforming input data into a desired output, based on specified calculations' (Gillespie, 2014: 167).[1] Altogether, these works point to a shift towards what Rouvroy and Berns (2013; also Rouvroy, 2013) call 'algorithmic governmentality': a governance steered by learning machines and intelligent computing systems that are able to automatically capture and process data from multiple sources, using statistical calculations that humans and socio-political institutions are by and large no longer able to understand and master.

Yet, an analytics of data protection highlights that these critical approaches tend to overlook the role played by other elements populating and enacting data-driven governance, notably digital data. *Digital data* are translations of people, things, behaviours and relations, into information that can be stored, computed and visualized by computers (see also Hansen, 2015; Kitchin, 2014; Lupton, 2015).[2] The argument underpinning this article is that a critical approach to the socio-political fabric of the digital (and *a fortiori* that of algorithmic governmentality) requires a better understanding of how digital data come to matter and how they are governed. This is not simply because 'digital tools facilitate datafication greatly' (Mayer-Schönberger and Cukier, 2013: 191), but, more importantly, because we (humans) and digital data (be they personal, meta- or derivative) are continuously entangled in socio-technical assemblages (Amoore, 2011; Aradau and Blanke, 2015; Dalton and Thatcher, 2014; Kitchin, 2014). And an analysis of data protection, and especially of its shortcomings, invites us to think about digital data beyond classical notions of data as representations of human subjects (Matzner, 2016). Borrowing from Haraway's work on the need to find an appropriate relation with non-humans (Haraway, 2008), Lupton has recently suggested that digital data are our 'companion species that have a life of their own that is beyond our complete control' (Lupton, 2016: 3). Their production, processing and simple existence may affect us, which in turns means that the question of how they are governed matters also for the way in which we are governed (Cardon, 2013; 2015). Hence, the overall ambition of this article is to feed into the scholarly debates about algorithmic governmentality by showing that *protecting* digital data is both of governmental *and* of political relevance. Moreover, studying the politics of data protection is a way to problematize once again the seemingly mundane, and often obscure, practices of collecting, storing, exchanging, processing, pseudonymizing or anonymizing digital data.

The article is structured into two main sections. In the first section, it clarifies my conceptual approach, explaining the most relevant tenets of governmentality studies and Actor-Network-Theory. It then discusses how these literatures can contribute to a study of data-driven governance, and in particular of data protection as a form of internal critique to the politics of the 'digital age'. It presents the conceptual tool of *dispositifs*, which are defined by Foucault as both operators of power and grids of analysis (Foucault, 1980 [1977]). It also introduces the analytical distinction between *politics* and *political* (Barry, 2002), the former including techniques, institutions and expertise, and the latter signalling the possibility of disagreement. In the second section, the article ventures, equipped with *dispositifs* as a conceptual tool, into an analytics of data protection and some of its configurations. It starts by introducing data protection as a loose set of material, legal and organizational elements that can be mobilized by socio-political actors. Then it examines the emergence, and tentative stabilization, of *data protection by design and by default*, i.e. a project to ensure the respect of personal data protection through the adoption of tailored technological and organizational systems. The data protection reform has recently translated this ambition into EU legislation. An analysis of the different conceptualizations of the same project permits us to assess how data protection may help both humans and digital data not to be algorithmically governed *like that*.

Governmentality, dispositifs, politics

The word *governmentality* is a neologism introduced by Foucault during his lectures at the Collège de France in the late 1970s. In the lecture of 1 February 1978, he explained that, with 'this word' he was referring to both a historical 'tendency', traceable back to at least the fifteenth and sixteenth centuries, and a somewhat specific way of organizing power in the West, where diverse techniques, forms of knowledge and theorization support and limit the act of governing people and things (Foucault, 2009: 108–9). This lecture was published as a stand-alone piece (e.g. Foucault, 2003a) well before the release of the entire course (Foucault, 2009). It quickly became a seminal reference for those researchers analysing the practice and the rationality of governing through its discontinuities, in particular, in relation to the role played by the state in the second half of the twentieth century (*inter alia* Rose, 2004 [1999]). For example, Rabinow and Rose explain that:

> Foucault initially forged the concept of 'governmentality' in an attempt to understand the characteristics of liberalism as a mentality of government that started from the presupposition that society existed external to the state, and constrained itself by limiting the scope of legitimate power, subjecting it to a range of constraints, and constantly requiring it to justify itself. (Rabinow and Rose, 2003: x)

Similarly, Walters emphasizes the added value of studying power relations in terms of governmentality:

> [t]his tool-box equips us to do something important and quite novel: to understand governance not as a set of institutions, nor in terms of certain ideologies, but as an eminently practical activity that can be studied, historicised and specified at the level of the rationalities, programmes, techniques and subjectivities which underpin it and give it form and effect. (Walters, 2012: 2)

The study of governmentality has, since Foucault's work on statistics, been particularly interested in how the organization of power is mediated by technologies of control based on the collection and processing of records (e.g. Foucault, 2009). Governmentality studies have shown how numbers (Rose, 2004 [1999]), indicators (Walters and Haahr, 2005) and other means of quantification, such as accounting and benchmarking (Miller and Rose, 2008) lie at the very heart of the art of governing people and things. The influence of governmentality can also be traced in the approach of Actor-Network-Theory (Akrich et al., 2006; Latour, 2005; Law and Hassard, 1999), which invites researchers not to undervalue the role played by technologies (and other non-humans) in the making of society and in the endeavour to stabilize power relations (Callon and Latour, 1981). In turn, this ontological view – where both humans and non-humans are to be studied not as mere instruments but rather as mediators and co-producers of the world they inhabit – has also influenced the governmentality literature (e.g. Barry, 2001).

From this perspective, a governmentality approach seems a particularly apt theoretical foundation to help understand data-driven governance. This means, in terms of theoretical guidance, studying specific data-driven practices, focusing in particular on

how diverse actors – be they human or non-human – and forms of knowledge and expertise, come to disturb, criticize, influence or stabilize a given mode of governing. For example, several scholars are currently focusing on algorithms and are unpacking the implications of their governing force on the practice and conceptualization of democracy (Crawford, 2016), of identity (Cheney-Lippold, 2011), of citizenship (Isin and Ruppert, 2015), of science (Pontille and Torny, 2013), of culture (Hallinan and Striphas, 2016), or of security (Bauman et al., 2014), etc.

A governmentality approach to the digital and its politics can also be extended to the study of data protection, which can be seen as a crucial form to problematize both the will to *govern through data* and the will to *govern data*. Eventually, this may contribute to bringing to critical scholars' attention, the role of digital data in shaping digital governance. As Kitchin elegantly puts it, data share the fate of 'bricks and mortar' (2014: 1). Actors and researchers consider them as foundational, but ultimately mundane, elements of greater assemblages: their conditions of generation (Thatcher et al., 2016) and the labour of making them 'algorithm-ready' remain largely overlooked (Gillespie, 2014: 171).

The 'fundamental right' facet of data protection, and more generally its socio-legal predominant character, do not make it less relevant in terms of governmentality. Here, I follow Golder's (2015) study analysing Foucault's interest in human rights in its late works. He notes that, for Foucault, '[r]ights do present themselves as one of a range of contingent political tools available for counter-investment and appropriation, for "strategic reusability" on behalf of different political interests and as a part of diverse political struggles' (Golder, 2015: 22). As such, they are not a vestige of a rationality and mode of government left behind by the incessant process of governmentalization, but rather are an integral and potentially influential part of power relations: an important form of critical counter-conduct (Golder, 2015).

Both the governmentality literature and Actor-Network-Theory offer a valuable conceptual tool: *dispositifs*. For Foucault, dispositifs are 'strategies of relations of forces supporting, and supported by, types of knowledge' (1980 [1977]: 196), which can be transformed into an important methodological device for apprehending forms of governmentality (Rabinow and Rose, 2003; Thomas, 2014). Actor-Network-Theory scholars similarly refer to *settings* (Akrich and Latour, 1992: 259), *work-nets* (Latour, 2005: 132) and *method-assemblage* (Law, 2004: 161). Generally speaking, this conceptual instrumentation enables the researcher to sketch tentative descriptions of research objects where agency is not exclusively located in either human or non-human elements, but can rather be found in their continuous interaction (Latour, 1999). Acuto and Curtis call this ontological and methodological take 'assemblage thinking' and note that:

> the very genesis of 'assemblage thinking' as a *modus operandi* for the social sciences brings evidence of this way of operating, being itself a composite of complex and diverse ideas coming from political philosophy, sociology and STS, making up for a theory of assemblages that is itself an assemblage of views and methods. (Acuto and Curtis, 2014: 9)

When it comes to the digital, big data and mass surveillance, scholars tend to use the conceptual tool of dispositifs, or assemblage, mainly in relation to algorithms and other

data-driven technologies (Aradau and Blanke, 2015; Bellanova and Duez, 2012; Bigo, 2008; Haggerty and Ericson, 2000; Jacobsen, 2012; Thomas, 2014), rather than in relation to research objects that are, *prima facie*, marked by their socio-legal elements (a notable exception being: Pottage, 2012). Yet, it is heuristically promising to use dispositifs beyond their more common 'application' to socio-technical systems. In this article, this means to approach data protection and data protection by design like any other instance of data-driven governance, for example, socio-technical surveillance systems like body scanners or drones. Actually, data protection has a very heterogeneous composition, including fundamental rights, legislation, case-law, ad hoc regulatory institutions, data protocols, and many other elements. As such, any tentative description of what data protection is could be read as a textbook example of what has become a seminal definition of *a* dispositif: 'a thoroughly heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions' (Foucault, 1980 [1977]: 194).

As other researchers have noted (e.g. Bonditti, 2012), the notion of the dispositif is fascinating because it resonates with the problem of understanding the relations between multiplicity and action. Yet, the problem with dispositifs is that any comprehensive description of what a dispositif *is* seems to potentially extend *ad libidum*, leaving no exteriority to the same. At the same time, focusing only on a very specific set of elements triggers the risk of missing out some crucial discordances and thus somewhat paradoxically reifying the black-box*ness* of research objects. To escape this potential deadlock, Walters suggests that researchers ask themselves, 'What is not a dispositif?' (2012: 77). And as a rule of thumb, he proposes respecting an 'analytical distinction between apparatus and assemblage' (Walters, 2012: 77). Apparatuses would then refer to stabilized multiplicities, and assemblages to heterogeneous ensembles still in flux, which 'either crystallize into apparatuses; or they fragment and disappear' (Walters, 2012: 77). This trick of the trade may be useful, but its assumption of a one-way progressive evolution from assemblages to apparatuses does not seem to work well when it comes to cases in which dispositifs remain highly contested and their potential stabilization around a specific configuration is a continuous matter of negotiation. And so, in the next section, I will refer to a *reservoir-dispositif* whenever the dispositif is described in terms of a (contested) list of elements and its overall – somehow institutionalized – rationality. And, I will refer to *specific dispositifs* when actors put forward specific arrangements of data protection elements and load them with a strategic purpose.

Before moving on to the more analytical section of this article, I want to present another vantage point with the theoretical guidance of governmentality literature. Governmentality seems to mark the end of any externality or radical alternative: and indeed, critique seems to be perceived to be operating from within (Cadman, 2010; Hansen, 2016). According to Latour, debunking critique is of no use in order to understand the world we inhabit and/or to protect what matters to each actor (Latour, 2004). However, this does not mean that the political dimension is doomed to fail and that socio-political actors will straightforwardly implement technologies of governance without meeting any kind of resistance (O'Malley et al., 1997). In actual fact, the focus of both governmentality studies and Actor-Network-Theory on practices of counter-conduct (Golder, 2015), knowledge

controversies (Barry, 2012) and the like, shows that a continuous tension between agreement and disagreement underpins power relations and socio-technical assemblages. Barry's work is of particular relevance, because it proposes an analytical distinction between *politics* and *the political* to better grasp the socio-political fabric of governmentality (Barry, 2002). Politics is 'a set of technical practices, forms of knowledge and institutions' – which are themselves the result of conflicts and agreements, whereas the political is 'an index of the space of disagreement' (Barry, 2002: 270). And where this space of disagreement is foreclosed by a specific kind of politics, these techniques or institutional arrangements have an *anti-political* character (Barry, 2002: 270).

Both the insight about the capacity of socio-political actors to re-appropriate techniques of government, and the distinction between politics and the political are in stark contrast to an ontological description of data-driven governance, where algorithms would leave little to no room to manoeuvre to a politics able to preserve the political (Berry, 2014; Rouvroy, 2013; Supiot, 2015). For instance, Ziewitz has suggested calling this worldview an 'algorithmic drama' where algorithms are presented as both powerful and opaque, and where ultimately this 'opacity of operation tends to be read as another sign of influence and power' (2016: 5–6). In the following section I will try to move beyond this drama and investigate how the rule and opacity of algorithms are challenged, or preserved, by data protection.

From data protection to data protection by design and by default

Data protection is many things. For instance, Gutwirth and De Hert define data protection as 'a catch-all term for a series of principles with regard to the processing of personal data' (2008: 281). However, it is more than a series of principles, and the conceptual tool of dispositif permits us to pinpoint some of its core elements. Many things can be considered socio-legal devices: a fundamental right (enshrined in Article 8 of the EU Charter), European legal instruments, national legislation, jurisprudence at national and European level (both the European Court of Human Rights and the EU Court of Justice) (Bygrave, 2002; González Fuster, 2014; Gutwirth et al., 2009). Other similar elements are the legal and policy-making practices, in particular, the policy-making implications of Article 16 of the Treaty on the Functioning of the EU and the 'proportionality test' derived from the text of Article 8 of the European Convention of Human Rights and its case law (Bagger Tranberg, 2011; González Fuster and Gellert, 2012). The data protection reservoir-dispositif includes also a bulk of national and European institutions: national regulatory authorities (i.e. Data Protection Authorities), an EU institution (the European Data Protection Supervisor), and a *sui generis* EU actor, the so-called Article 29 Working Party, a sort of spokesperson for national data protection authorities (Hijmans, 2006; Poullet and Gutwirth, 2008). There is also a growing number of data protection experts, generally called privacy or data protection officers, whose function is to provide in-house advice and supervision.

Data protection enacts two forms of subjectivities: *personal data* and *data subjects*. Actually, the main target of governing in the case of data protection is personal data, which are generally understood as 'any information relating to an identified or

identifiable natural person' (Article 2a, EU Data Protection Directive). This means that the reach of data protection formally does not coincide with the full spectrum of the digital, but only with those digital data that are produced and processed in a way that permits establishing a relation with a natural person. Indeed, the continuous spread of digital technologies and the continuous generation of metadata trigger controversies over the validity and the political effects of a reductive reading of the definition of personal data. Data subjects are somehow a secondary and derivative form of subjectivity fostered by data protection: individual citizens and human beings become 'relevant' only insofar as they can be constructed as data subjects. In the European legal jargon, a data subject is: 'an identifiable person . . . who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his [*sic*] physical, physiological, mental, economic, cultural or social identity' (Article 2a, EU Data Protection Directive).

Finally, new elements such as data protection by design, are emerging on the periphery of data protection practices and regulatory frameworks. I discuss some of them more extensively below. For now, it is sufficient to say that these new elements can be described as tailored solutions that permit the deployment of data protection without (continuously) mobilizing the full array of data protection instruments.

Further, not all the elements of this continuously growing reservoir-dispositif are mobilized at the same time, and different actors build *their* specific data protection dispositif in diverse ways. Hence, presenting data protection as a reservoir-dispositif allows us to convey the idea that there is not a definite list of what constitutes data protection, and that data protection can be seen rather as a provider of socio-legal and technical devices that actors can (try to) enlist and mobilize. Moreover, speaking about data protection in terms of reservoir-dispositif rather than apparatus highlights the fact that data protection is not something that has been stabilized once and for all. Its scope and strategic objectives are a matter of continuous confrontation and elaboration, and this has recently been emphasized by the wealth of amendments (circa four thousand) presented during the data protection reform.

According to Foucault, each dispositif has a 'dominant strategic function' (1980 [1977]: 194). In the case of data protection, it has historically been two-fold: 'the protection of individuals with regard to the processing of personal data' and 'the free movement of such data', as stated in the very title of the EU Data Protection Directive. This double strategic function contributes to a proliferation of diverse versions of the data protection dispositif, that are not always consistent in terms of intentionality. Yet, it also formally grants to the data protection reservoir-dispositif a remarkable level of flexibility, as the analysis below on data protection by design highlights. This double strategic function also implies that the human right to privacy had to be regulated and tamed so as to favour societal evolution towards digital-friendly markets and governmental practices. And indeed, vice versa, new technologies have to be able to foresee and afford the interaction with individuals turned into data subjects.

The data protection reform, together with the recent scandal about secret mass surveillance programs, has furthered the tension between the two strategic objectives of data protection. On paper, data protection by design seems to finally offer a way of reconciling both: it promises a seamless governance of digital data to the mutual benefits of data

subjects and big data enthusiasts – be they corporations or state authorities (D'Aquisto et al., 2015). Yet, an analytics of its emergence in the EU framework allows us to appreciate how conceptualizing data protection by design can bring to different specific data protection dispositifs with their own sets of politics and political implications.

In the remainder of the section, I briefly analyse three of the main practices and discourses that lie at the root of data protection by design as well as the governmental ambitions and contestation surrounding its inscription into the EU legal framework.

As noted by Rubinstein, '[p]rivacy by design is an amorphous concept' (2011: 1421): there is no unique understanding or stabilized definition. A minimalistic view is that privacy by design happens when the attentive implementation of data protection principles is embedded in the design of a new technology. A more comprehensive view is that privacy by design can be only achieved if a series of regulatory, technical and organizational measures are actively followed through the entire life-cycle of practices based on technologies. A popular conceptualization of privacy by design has been proposed by the former Information and Privacy Commissioner of Ontario, Ann Cavoukian (Danezis et al., 2014). According to her work, privacy by design implies the application of fair information principles, such as transparency and data security, whenever personal information (i.e. personal data) are at stake. Initially presented in the early 1990s, these principles have only been marginally adapted to the introduction of new technologies, including big data processing (cf. Cavoukian and Jonas, 2012). The formulation of privacy by design through these principles can be read as the generation of a specific data protection dispositif, which comes with a politics aimed at orientating data protection towards a mix of IT security and risk management techniques (Spiekermann, 2012a). This specific data protection dispositif risks contributing to the foreclosure of the political space, because it would protect actors that are able to process massive amounts of digital data from any further political contestation of their doings. So far, this kind of privacy by design has not reached a consensus and has become in itself a field of political confrontation. Several legal experts and computer scientists have contested the effective value of these principles, or even the possibility of their application (Gürses et al., 2012; Le Métayer, 2010; Rubinstein, 2011; Rubinstein and Good, 2013).

Another important element at the root of data protection by design is *Privacy Enhancing Technologies* (PETs). PETs' own history lies in computer science and cryptology (Danezis et al., 2014): they are technologies that explicitly aim at protecting informational privacy. Rubinstein proposes a 'taxonomy of PETs' where these technologies are divided into two main groups: 'substitutes' and 'complements' (Rubinstein, 2011: 1417ff.). Rubinstein's taxonomy is useful because it highlights that not all technological solutions have the same political ambition. On the one hand, substitutes PETs aim at ensuring anonymity, which is a somewhat radical version of data protection: users can exploit some digital services (i.e. web browsers or electronic ticketing systems) without exposing themselves to surveillance while, de facto, contesting the very surveillance rationale underpinning the provision of these services. On the other hand, complements PETs are to be considered technological fixes that ensure, or merely show, compliance with relevant privacy or data protection legislation, without contesting or challenging the logistics of surveillance created by many digital systems. From this perspective, privacy

enhancing technologies may relate the digital to politics either politically (in the case of substitutes PETs) or anti-politically (in the case of complements PETs).

A third key element for data protection by design are *Privacy Impact Assessments* (PIAs). Privacy Impact Assessments had already been developed in the 1990s in several Anglo-Saxon countries (Wright and De Hert, 2012), and can be defined as 'a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme' (Clarke, 2011: 111). Their conceptual background is the development and diffusion of impact assessment methods and approaches, from environmental impact assessments to technological impact assessments (Wright and De Hert, 2012). PIAs methodologies generally foresee the participation of both proponents of a new measure and those that will be affected, often represented by experts, advocates and public institutions. In this sense, PIAs may be considered a type of data protection dispositif offering the most in terms of political space of contestation. They invite diverse socio-political actors to actively participate in the definition of technologies and influence the tentative agreement. The potential here is that data protection can open a space of contestation that focuses not only on privacy and data protection compliance, but also on other issues at stake in data-driven governance, such as discrimination, information asymmetries, labour conditions, etc.

Yet, the case concerning the assessment of the possible impact of Radio-Frequency Identification (RFID) technologies on fundamental rights (European Commission, 2009) shows how fragile specific data protection dispositifs can become. RFID are systems composed of tags storing information, and readers able to access and read that information remotely. A classic example is public transport cards with chips holding data about tickets and their owners, that can be used to open automatic gates or that can be checked or scanned in case of ticket controls. RFID are widely used in several sectors, from logistics to retail and access control, and their potential in terms of surveillance is quite evident (Marlin-Bennett, 2016). In January 2011, the European Commission gave the green light to the 'Privacy and Data Protection Impact Assessment Framework for RFID Applications', conceived by private companies active in the RFID business. This PIA framework is heavily reliant on a risk assessment logic, which also includes a pre-assessment phase to identify whether there is a need for a full-scale PIA. Furthermore, even if privacy risks are identified, a series of measures are suggested to mitigate them, both at the stage of design and implementation. This case shows that the political potential of PIAs can be severely reduced when they are implemented and translated into a framework that does not require the active participation of the wider public. Then, the only political possibility left is that of contesting the validity of the PIAs framework itself (Spiekermann, 2012b).

The term *data protection by design and by default* was first introduced by the European Commission in its two proposals aiming at reforming the EU legislative framework on data protection (cf. in particular, European Commission, 2012). And, following the adoption of the two new EU legal instruments (European Parliament and Council, 2016a; 2016b), it is now inscribed into the data protection reservoir-dispositif. The ostensible program of data protection by design and by default is to embed data protection principles and objectives in the very core of data collection and processing, thereby anchoring a regulative device directly into organizational and technological practices. The ambition of the EU institutions is to morph data protection into a specific dispositif

that can be pushed upon, and enacted by, the socio-technical actors processing data. As such, data protection by design would be a powerful way to govern data, and by extension the everyday making of the digital.

However, a closer reading of the provisions hint at the weakness of these data protection politics, at least insofar as they will not be further translated by other actors into more detailed technologies and organizational routines. Indeed, instead of enacting specific and substantial standards, data protection by design and by default deploys itself as a legal device with a strong procedural approach. For example, it forces data controllers – as the socio-technical actors defining the goals and the means of harvesting and processing digital data are called – to think about data protection when developing data-driven technologies, and to 'implement appropriate technical and organizational measures' (European Parliament and Council, 2016b: Article 25). However, besides mentioning pseudonymization as an appropriate technique, no clear standards are brought forward. As seen above for the case of PIAs, much will depend on how institutions, corporates and experts will be able to influence the setting-up of specific standards.

When it comes to data protection by default, its political potential resides mainly in the obligations for data controllers to set up a technical and organizational system that 'shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons' (European Parliament and Council, 2016b: Article 25). This seems to bring the data subjects back into a control position over data-driven governance, but it risks remaining a void position if we take seriously the growing shift towards producing digital data that are de-linked from data subjects, for example, in the cases of pseudonymized, mosaic or aggregated data (Amoore, 2013: 84ff.; van Otterlo, 2013).

In fact, somewhat paradoxically, data protection by design and by default risks bringing to a breaking point the grasp of data protection on data-driven governance. The General Data Protection Regulation, the most comprehensive in scope and reach of the two new EU legal instruments, seems to prevent this crashing point, by introducing two different definitions for pseudonymized and anonymized data (European Parliament and Council, 2016b: para. 26). While anonymized data should not be concerned by the scope of data protection because 'the data subject is not or no longer identifiable' (*idem*), pseudonymized data remain to be considered, in principle, personal data. However, the heuristics used to justify the difference between pseudonymized and anonymized data remain premised on the rationale that it should be 'reasonably' doable to re-associate the pseudonymized data to a given individual (cf. also Article 29 WP, 2007). This implies that some pseudonymized data can eventually end up not being protected because their re-personalization would be deemed too challenging.

Here, this brief analytics of the emergence of data protection by design and by default points towards the main epistemic and political limit of the data protection reservoir-dispositif. The two forms of subjectivities that it generally produces – personal data and data subjects – remain meaningful only in order to grasp and question a part of data-driven governance. Nowadays, profiling systems mostly work with data at the 'aggregated level', from which they produce profiles that 'provide means to *infer* knowledge about an individual who is not actually observed' (van Otterlo, 2013: 43–4, italics in original). While aggregated data have somewhere to be initially collected – and at that

point in time they are personal data – once they are ingested, they largely can be anonymized. The governing ambition of this type of algorithms does not rest on the *identification* of people: '[i]nstead, the profile is *applied to* the individual user to infer additional facts, preferences or assumed intentions (e.g. to buy certain product)' (van Otterlo, 2013: 44, italics in original). These are the profiling systems that populate and ultimately characterize the landscape of Rouvroy and Berns' algorithmic governmentality (Rouvroy and Berns, 2013).

From this perspective, the 'personological approaches' to data protection, as well as '[t]ransparency enhancing technologies [and] privacy enhancing technologies' provide no ground to seriously criticize and counter algorithmic governmentality (Rouvroy, 2013: 159), and critique can only emerge from a 'space of common appearance within which we [human beings] are mutually addressed to each other' (Rouvroy, 2013: 159–60). Yet, even if all data protection dispositifs are doomed to fail in contesting frontally algorithmic governmentality, some of them give us the means to disrupt the 'dramatic staging' of algorithms as perfectly sealed black-boxes, and hint at the need to find more appropriate ways to relate to digital data as companion species rather than treating them as either our property or mere leverages of social control.

Conclusion

This article has argued that the relation between the digital and politics can aptly be investigated through the lens of data protection. This is what many actors have been doing since the late 1960s, whether it be to contest or support specific forms of data-driven governance (Bennett and Raab, 2006). This does not mean that data protection functions as the magic solution to controversial issues such as mass surveillance or big data technologies. Still, data protection remains one of the possible ways to intervene in order to not be algorithmically governed *like that*.

In particular, data protection invites us to widen the analytical focus so as to include not only 'governing algorithms' (Ziewitz, 2016) but also digital data. The role of these seemingly mundane elements in the landscape of algorithmic governmentality remains largely overlooked (with few exceptions: Gillespie, 2014; Gitelman and Jackson, 2013; Thatcher et al., 2016). Data protection reminds us that *governing through data* implies, first and foremost, *governing data*. Moreover, starting with data protection contributes to fostering an academic and political approach to digital data where data are 'an object of inquiry rather than subsumed to knowledge' (Aradau and Blanke, 2015: 9), and where data are 'matters of concern' rather than 'matters of fact' (Latour, 2004: 231).

An analytics of data protection dispositifs, and in particular when configured as data protection by design and by default, has also shed light on some of its political and epistemic limits. Many data protection dispositifs are more prone to supporting data-driven governance than to fostering a political space of disagreement. Moreover, data protection is limited when it comes to retaining a grasp on, and to protecting, digital data that are not personal data. This is increasingly problematic in a present marked by the proliferation of profiling systems that affect us through the computation of data to which we retain no direct or *personal* relation, at least in data protection terms. The ambition of large-scale data processors is to crunch *big* data but to operate with little to no *personal*

data (Cheney-Lippold, 2011). This may sound like a 'world that algorithms dream of' (to borrow from Cardon, 2015: 8, author's own translation), and, as such, far from the actual everyday experience of the digital by users (Gillespie, 2014). Still, it raises the crucial question of what relations we can, and want to, establish with our 'digital companion species' (Lupton, 2016: 1). While this article has highlighted some of the limitations that render data protection poorly equipped to address this question *politically*, it has also shown that data protection is deeply entwined into the *politics* of algorithmic governmentality. Hence, it remains worth investigating the political purchase of diverse data protection dispositifs, and following their everyday doings, and this, from a governmentality perspective.

Acknowledgements

I am grateful to Mareile Kaufmann, Julien Jeandesboz and Heidi Mercenier for their comments and patience. Thanks to Raphaël Gellert, Darek Kloza and Denis Duez for our conversations on algorithms, data protection and governmentality, and to Bertrand Lescher-Nuland for proofreading the manuscript.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The research has been carried out with the economic support of the following research projects: Actions de recherche concertées (ARC) – 'Why Regulate? Regulation, De-Regulation and Legitimacy of the EU' (funded by the Communauté française de Belgique); and NordSTEVA – 'Nordic Centre for Security Technologies and Societal Values' (funded by NordFORSK).

Notes

1. Algorithms, their agency and their role in the governance of contemporary societies are currently at the centre of scholarly conversations in several fields of social sciences and humanities, with special issues announced or already released by journals as diverse as *Science, Technology & Human Values* (Governing Algorithms, 2016), *Security Dialogue* (Security with Algorithms, 2017), *Philosophy and Technology* (The Governance of Algorithms, 2017) and *Information, Communication & Society* (The Social Power of Algorithms, 2017).
2. Obviously, this definition of digital data should not be read as including all possible kinds of data. According to Kitchin (2014: 1): '[d]ata are commonly understood to be the raw material produced by abstracting the world into categories, measures and other representational forms – numbers, characters, symbols, images, sounds, electromagnetic waves, bits – that constitute the building blocks from which information and knowledge are created.' This article focuses on the digital and thus, for the sake of clarity, when the word 'data' is used, it should be understood only in the more limited sense of digital data.

References

Acuto M and Curtis S (2014) Assemblage thinking and international relations. In: Acuto M and Curtis S (eds) *Reassembling International Theory*. Basingstoke: Palgrave, pp. 1–15.

Akrich M, Callon M and Latour B (eds) (2006) *Sociologie de la traduction*. *Textes fondateurs*. Paris: Les Presses Mines ParisTech.

Akrich M and Latour B (1992) A summary of a convenient vocabulary for semiotics of human and nonhuman assemblies. In: Bijker W E and Law J (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press, pp. 259–64.

Amicelle A, Aradau C and Jeandesboz J (2015) Questioning security devices: performativity, resistance, politics. *Security Dialogue* 46(4): 293–306.

Amoore L (2011) Data derivatives: on the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28(6): 24–43.

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability*, London: Duke University Press.

Amoore L and de Goede M (2012) Introduction: data and the war by other means. *Journal of Cultural Economy* 5(1): 3–8.

Andrejevic M and Gates K (2014) Big Data surveillance: introduction. *Surveillance & Society* 12(2): 185–96.

Aradau C and Blanke T (2015) The (Big) Data-security assemblage: knowledge and critique. *Big Data & Society* 2(2): 1–12.

Article 29 WP (2007) Opinion 4/2007 on the concept of personal data. Brussels: Article 29 Data Protection Working Party.

Bagger Tranberg C (2011) Proportionality and data protection in the case law of the European Court of Justice. *International Data Privacy Law* 1(4): 239–48.

Barry A (2001) *Political Machines: Governing a Technological Society*. London: Athlone Press.

Barry A (2002) The anti-political economy. *Economy and Society* 31(2): 268–84.

Barry A (2012) Political situations: knowledge controversies in transnational governance. *Critical Policy Studies* 6(3): 324–36.

Bauman Z, Bigo D, Esteves P, et al. (2014) After Snowden: rethinking the impact of surveillance. *International Political Sociology* 8(2): 121–44.

Bellanova R and Duez D (2012) A different view on the 'making' of European security: the EU Passenger Name Record System as a socio-technical assemblage. *European Foreign Affairs Review* 17(2/1): 109–24.

Bennett C J (2008) *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Bennett C J and Raab C (2006) *The Governance of Privacy*. *Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Berry D M (2014) *Critical Theory and the Digital*. New York: Bloomsbury.

Bigo D (2008) Globalised (in)security: the field and the ban-opticon. In: Bigo D and Tsoukala A (eds) *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes*. London: Routledge, pp. 10–48.

Bonditti P (2012) Act different, think *dispositif*. In: Salter M B and Mutlu C E (eds) *Research Methods in Critical Security Studies: An Introduction*. London: Routledge, pp. 101–4.

boyd d and Crawford K (2012) Critical questions for Big Data: provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662–79.

Bygrave LA (2002) *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

Cadman L (2010) How (not) to be governed: Foucault, critique, and the political. *Environment and Planning D: Society and Space* 28(3): 539–56.

Callon M and Latour B (1981) Unscrewing the big Leviathan: how actors macro-structure reality and how sociologists help them to do so. In: Knorr-Cetina K D and Cicourel A V (eds) *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*. Boston: Routledge & Kegan Paul, pp. 277–303.

Cardon D (2013) Dans l'esprit du PageRank. Une enquête sur l'algorithme de Google. *Réseaux* 177(1): 63–95.

Cardon D (2015) *À quoi rêvent les algorithmes?* Paris: Seuil.

Cavoukian A and Jonas J (2012) *Privacy by Design in the Age of Big Data*. Toronto: Information and Privacy Commissioner Ontario.

Cheney-Lippold J (2011) A new algorithmic identity: soft biopolitics and the modulation of control. *Theory, Culture & Society* 28(6): 164–81.

Chun WHK (2011) *Programmed Visions: Software and Memory*. Cambridge, MA: MIT Press.

Clarke R (2011) An evaluation of privacy impact assessment guidance documents. *International Data Privacy Law* 1(2): 111–20.

Crawford K (2016) Can an algorithm be agonistic? Ten scenes from life in calculated publics. *Science, Technology, & Human Values* 41(1): 77–92.

Dalton C and Thatcher J (2014) What does a critical data studies look like, and why do we care? Seven points for a critical approach to 'big data'. *Society & Space*. Available at: http://societyandspace.com/material/commentaries/craig-dalton-and-jim-thatcher-what-does-a-critical-data-studies-look-like-and-why-do-we-care-seven-points-for-a-critical-approach-to-big-data/

Danezis G, Domingo-Ferrer J, Hansen M, et al. (2014) *Privacy and Data Protection by Design: From Policy to Engineering*. Heraklion: ENISA.

D'Aquisto G, Domingo-Ferrer J, Kikiras P, et al. (2015) *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*. Heraklion: ENISA.

Dean M (1999) *Governmentality: Power and Rule in Modern Society*, London: SAGE.

EP Press Service (2016) Data protection reform: Parliament approves new rules fit for the digital era. Strasbourg: European Parliament.

European Commission (2009) Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Brussels: European Commission.

European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final. Brussels: European Commission.

European Parliament and Council (2016a) Directive (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation,

detection or presecution of criminal offences or the execution of criminal penalities, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Luxembourg: Official Journal of the European Union.

European Parliament and Council (2016b) Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Luxembourg: Official Journal of the European Union.

Foucault M (1980[1977]) The confession of the flesh. In: Gordon C (ed.) *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*. New York: Pantheon Books, pp. 194–228.

Foucault M (2003a) Governmentality. In: Rabinow P and Rose N (eds) *The Essential Foucault: Selections from Essential Works of Foucault, 1954–1984*. New York: The New Press, pp. 229–45.

Foucault M (2003b) What is critique? In: Rabinow P and Rose N (eds) *The Essential Foucault: Selections from Essential Works of Foucault, 1954–1984*. New York: The New Press.

Foucault M (2009) *Security, Territory, Population: Lectures at the Collège de France, 1977–1978*. New York: Picador/Palgrave Macmillan.

Gillespie T (2014) The relevance of algorithms. In: Gillespie T, Boczkowski P J and Foot K A (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press, pp. 167–93.

Gitelman L and Jackson V (2013) Introduction. In: Gitelman L (ed.) *'Raw Data' Is an Oxymoron*. Cambridge, MA: MIT Press, pp. 1–14.

Golder B (2015) *Foucault and the Politics of Rights*. Stanford, CA: Stanford University Press.

González Fuster G (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Dordrecht: Springer.

González Fuster G and Gellert R (2012) The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology* 26(1): 73–82.

Gürses S, Troncoso C and Diaz C (2012) *Engineering Privacy by Design*. Leuven: COSIC.

Gutwirth S and De Hert P (2008) Regulating profiling in a democratic constitutional state. In: Hildebrandt M and Gutwirth S (eds) *Profiling the European Citizen: Cross-disciplinary Perspectives*. Dordrecht: Springer, pp. 271–91.

Gutwirth S, Poullet Y and De Hert P (eds) (2010) *Data Protection in a Profiled World*. Dordrecht: Springer.

Gutwirth S, Poullet Y, De Hert P, et al. (eds) (2009) *Reinventing Data Protection?* Dordrecht: Springer.

Haggerty K D and Ericson R V (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–22.

Hallinan B and Striphas T (2016) Recommended for you: The Netflix Prize and the production of algorithmic culture. *New Media & Society* 18(1): 117–37.

Hansen H K (2015) Numerical operations, transparency illusions and the datafication of governance. *European Journal of Social Theory* 18(2): 203–20.

Hansen M P (2016) Non-normative critique: Foucault and pragmatic sociology as tactical repoliticization. *European Journal of Social Theory* 19(1): 127–45.

Haraway D J (2008) *When Species Meet*. Minneapolis: University of Minnesota Press.

Hijmans H (2006) The European data protection supervisor: the institutions of the EC controlled by an independent authority. *Common Market Law Review* 43(5): 1313–42.

Hood C C and Margetts H Z (2007) *The Tools of Government in the Digital Age*. New York: Palgrave.

Introna L and Wood D (2004) Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance & Society* 2(2/3): 177–98.

Isin E F and Ruppert E (2015) *Being Digital Citizens*. London: Rowman & Littlefield.

Jacobsen E K U (2012) Unique identification: inclusion and surveillance in the Indian biometric assemblage. *Security Dialogue* 43(5): 457–74.

Kitchin R (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. London: Sage.

Kitchin R and Dodge M (2011) *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press.

Latour B (1986) The powers of association. In: Law J (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* London: Routledge, pp. 264–80.

Latour B (1999) *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press.

Latour B (2004) Why has critique run out of steam? From matters of fact to matters of concern. *Critical Inquiry* 30(2): 225–48.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. New York: Oxford University Press.

Law J (2004) *After Method: Mess in Social Science Research*. London: Routledge.

Law J and Hassard J (eds) (1999) *Actor Network Theory and After*. Oxford: Blackwell.

Leese M (2014) The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* 45(5): 494–511.

Le Métayer D (2010) Privacy by design: a matter of choice. In: Gutwirth S, Poullet Y and De Hert P (eds) *Data Protection in a Profiled World*. Dordrecht: Springer, pp. 323–34.

Lupton D (2015) *Digital Sociology*. London: Routledge.

Lupton D (2016) Digital companion species and eating data: implications for theorising digital data-human assemblages. *Big Data & Society* 3(1): 1–5.

Lyon D (2014) Surveillance, Snowden, and Big Data: capacities, consequences, critique. *Big Data & Society* 1(2): 1–13.

Marlin-Bennett R (2016) Everyday rules and embodied information: anti-money laundering/counter-terrorist financing practices and radio frequency identification tags as security politics. *Critical Studies on Security* 4(2): 169–86.

Matzner T (2016) Beyond data as representation: the performativity of Big Data in surveillance. *Surveillance & Society* 14(2): 197–210.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Eamon Dolan.

Miller P and Rose N (2008) *Governing the Present: Administering Economic, Social and Personal Life*. Cambridge: Polity Press.

O'Malley P, Weir L and Shearing C (1997) Governmentality, criticism, politics. *Economy and Society* 26(4): 501–17.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press.

Pontille D and Torny D (2013) La manufacture de l'évaluation scientifique. Algorithmes, jeux de données et outils bibliométriques. *Réseaux* 1(177): 23–61.

Pottage A (2012) The materiality of what? *Journal of Law and Society* 39(1): 167–83.

Poullet Y and Gutwirth S (2008) The contribution of the Article 29 Working Party to the construction of a harmonised European Data Protection System: an illustration of 'reflexive governance'? In: Pérez Asinari M V and Palazzi P (eds) *Défis du droit à la protection de la vie privée: Challenges of Privacy and Data Protection Law*. Brussels: Bruylant, pp. 569–607.

Raab C (1997) Co-producing data protection. *International Review of Law, Computers & Technology* 11(1): 11–24.

Rabinow P and Rose N (2003) Introduction. Foucault today. In: Rabinow P and Rose N (eds) *The Essential Foucault: Selections from Essential Works of Foucault, 1954–1984*. New York: The New Press, pp. vii–xxxv.

Regan PM (2012) Regulating surveillance technologies: institutional arrangements. In: Ball K, Haggerty K and Lyon D (eds) *Routledge Handbook of Surveillance Studies*. London: Routledge, pp. 397–404.

Rose N (2004 [1999]) *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.

Rose N and Miller P (1992) Political power beyond the state: problematics of government. *The British Journal of Sociology* 43(2): 173–205.

Rouvroy A (2013) The end(s) of critique. In: Hildebrandt M and de Vries K (eds) *Privacy, Due Process and the Computational Turn*. London: Routledge, pp. 143–67.

Rouvroy A and Berns T (2013) 'Gouvernementalité algorithmique et perspectives d'émancipation': Le disparate comme condition d'individuation par la relation? *Réseaux* 1(177): 163–96.

Rouvroy A and Poullet Y (2009) The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: Gutwirth S, Poullet Y, De Hert P, et al. (eds) *Reinventing Data Protection?* Dordrecht: Springer, pp. 45–76.

Rubinstein I S (2011) Regulating privacy by design. *Berkeley Technology Law Journal* 26(3): 1409–56.

Rubinstein I S and Good N (2013) Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal* 28: 1333–413.

Spiekermann S (2012a) The challenges of privacy by design. *Communications of the ACM* 55(7): 38–40.

Spiekermann S (2012b) The RFID PIA: developed by industry, endorsed by regulators. In: Wright D and De Hert P (eds) *Privacy Impact Assessment*. Dordrecht: Springer, pp. 323–46.

Supiot A (2015) *La Gouvernance par les nombres: Cours au Collège de France (2012–2014)*. Nantes: Fayard.

Thatcher J, O'Sullivan D and Mahmoudi D (2016) Data colonialism through accumulation by dispossession: new metaphors for daily data. *Environment and Planning D: Society and Space* 0(0): 1–17.

Thomas O D (2014) Foucaultian dispositifs as methodology: the case of anonymous exclusions by unique identification in India. *International Political Sociology* 8(2): 164–81.

van Otterlo M (2013) A machine learning view on profiling. In: Hildebrandt M and de Vries K (eds) *Privacy, Due Process and the Computational Turn*. London: Routledge, pp. 41–64.

Walters W (2012) *Governmentality: Critical Encounters*. New York: Routledge.

Walters W and Haahr J H (2005) *Governing Europe: Discourse, Governmentality and European Integration*. London: Routledge.

Wright D and De Hert P (eds) (2012) *Privacy Impact Assessment*. Dordrecht: Springer.

Ziewitz M (2016) Governing algorithms: myth, mess, and methods. *Science, Technology, & Human Values* 41(1): 3–16.

Author biography

Rocco Bellanova was earlier a Senior Researcher at the Peace Research Institute Oslo (PRIO), Oslo, Norway, and visiting lecturer at the Université Saint-Louis – Bruxelles (USL-B), Brussels, Belgium. His research focuses on digital data as pivotal elements in the governing of societies. He has carried out research on border security, passenger data surveillance, and data protection. He is currently affiliated with the University of Amsterdam (UvA), Amsterdam.