Original Research Article

BIG DATA & SOCIETY

Big Data & Society
July–December 2015: 1–12

DOI: 10.1177/2053951715609066
bds.sagepub.com
SAGE

The (Big) Data-security assemblage: Knowledge and critique

Claudia Aradau[1] and Tobias Blanke[2]

Abstract

The Snowden revelations and the emergence of 'Big Data' have rekindled questions about how security practices are deployed in a digital age and with what political effects. While critical scholars have drawn attention to the social, political and legal challenges to these practices, the debates in computer and information science have received less analytical attention. This paper proposes to take seriously the critical knowledge developed in information and computer science and reinterpret their debates to develop a critical intervention into the public controversies concerning data-driven security and digital surveillance. The paper offers a two-pronged contribution: on the one hand, we challenge the credibility of security professionals' discourses in light of the knowledge that they supposedly mobilize; on the other, we argue for a series of conceptual moves around data, human–computer relations, and algorithms to address some of the limitations of existing engagements with the Big Data-security assemblage.

Keywords

Big Data, security, critique computing and information science, assemblage, surveillance

Introduction

In the wake of the Snowden revelations, the question of how data is used for security purposes has re-emerged as a political problem. Critical inquiries around data and security are not new: from the production of traceability (e.g. Bonditti, 2008), proactive and pre-emptive management through data analytics (Aradau and van Munster 2011; Bigo, 2008; de Goede, 2012), database management, algorithmic governance or dataveillance in the 'war on terror' (Amoore and de Goede, 2005; Raley, 2013), the literature on security practices has analysed the multiple facets of the social and political transformations that the proliferation and increased use of data have entailed. The Snowden revelations and the emergence of 'Big Data' have rekindled these debates and prompted new inquiries into how digital practices and Big Data devices are deployed for the purposes of security and with what political effects.

These transformations have so far been analysed as part of the 'computational turn' in security governance, with data mining, predictive analytics and algorithmic decision-making playing an important role in the digital transformation of security (Amoore, 2011; Rouvroy, 2012). Big Data is an indicator of the transformations that digital information has brought about by being 'too big to know' (Weinberger, 2011). These dynamics have far-reaching implications for privacy and data protection, alongside civil liberties and human rights, which appear to be most at stake (Bauman et al., 2014; Lyon, 2014; Pasquale, 2015).[1] Therefore, critical scholars have concentrated mostly on social, political and legal challenges to Big Data and have paid less attention to the controversies around concepts and devices in computer and information science. The debates about the transformations that are underway have often tended to embrace particular dominant representations of this perceived computational or, more recently, Big Data 'revolution' rather than attending

[1]Department of War Studies, King's College London, Strand, London, UK
[2]Department of Digital Humanities, King's College London, Strand, London, UK

Corresponding author:
Tobias Blanke, Department of Digital Humanities, King's College London, 26-29 Drury Lane, Room 223, London WC2B 5RL, UK.
Email tobias.blanke@kcl.ac.uk

to the contestations and controversies about computing and digital knowledge formulated in these disciplines.

This paper investigates how the supposed 'novelty' implied by a digital transformation of security practices has been particularly put to use by security and intelligence experts in order to justify an urgent need for novel responses to anticipate and pre-empt the 'next terrorist attack'. For security professionals, Big Data, in particular, stands for the promise of solutions to contemporary security problems. Here, they are not so different from other institutional actors and strategies, from the development of e-science to new forms of e-government or a renewed focus in commercial organizations on their data assets. Critical scholars have similarly embraced this discourse of novelty in which Big Data is a 'game changer' (Hildebrandt, 2013: 8). We contend that these assumptions of novelty of a Big Data 'revolution' and game change in science – and by extension in governance practices – limit the potential of critical engagement. In analysing an emerging Big Data-security assemblage which brings together heterogeneous modes of knowledge, devices, institutions and methods, we address the impasses of critical discourses as formulated by civil liberties activists as well as critical scholars of security and Big Data.

Although the methods used by intelligence agencies like the National Security Agency (NSA) and Government Communications Headquarters (GCHQ) are secret, we start from the assumption that it is unlikely that their methods would be widely different from the state of the art in computing and information science, and the practices developed in dealing with Big Data in academic organizations and commercial institutions. In this sense, the paper understands intelligence agencies as Big Data organizations that employ data-driven methods to anticipate future dangers. A collaboration between social and computer scientists, as this paper proposes, can help go beyond the inscrutability of algorithmic methods in security practices.

In so doing, this paper develops a contribution to critical data studies (Kitchin, 2014) and critical approaches to security and surveillance (Amoore, 2014; Bauman et al., 2014; Lyon, 2014). We propose to take seriously the critical knowledge developed in information and computer science and reinterpret these debates to offer a critique of the common representations by security professionals of the digital transformation of their practices. The paper makes three moves that recast existing critical engagements with data-driven security: from data/metadata distinctions to the production of data as a complex epistemic entity; from a 'computational turn' in surveillance to the division of labour between humans and computers in socio-technical assemblages; from an underlying logic of algorithms to algorithmic practices and methods in security analytics.

These moves are developed through the analysis of three sites of public controversy about NSA and GCHQ surveillance and the use of Big Data for security governance in the wake of the Snowden revelations. The first controversy concerns the definition of digital data, and particularly the distinction between metadata and content, which has been used repeatedly by security professionals to justify bulk data collection. The second controversy we discuss relates to mass surveillance and the relationship between humans and machines in justifying surveillance practices. Here, a 'computational turn' in surveillance is used by security professionals as a reassurance that no privacy is invaded as only computers look at bulk-collected data. A third justification that security professionals have promoted is that they need to collect everything and make data big for algorithms to develop anticipatory knowledge of the 'next terrorist attack'. Contra these discourses of novelty, we show how debates in computer and information science can be mobilized to challenge the security professionals' claims to credible knowledge.

(Meta)data and the remaking of security knowledge

Since the Snowden revelations, a new concept has entered the public vocabulary: metadata. Long used by archivists and computer experts, metadata has more recently been at the heart of controversies about security practices. President Obama argued that the NSA programme was not gathering data but metadata, namely how long a call was or where it was made from. He reinforced that metadata collection would then be different from surveillance and proceeded to allay the public's fears: 'Nobody is listening to your telephone calls. That's not what this program is about' (Obama, 2013).

Metadata is therefore seen as not encroaching upon rights or privacy, as it does not reach content. In the UK, Theresa May has also claimed that privacy concerns only come into effect 'at the point at which the communication is opened' (Wheeler, 2014). Metadata is supposed to not convey information about what people say or do in their homes. In that sense, metadata is rendered as the opposite of the telephone tap and the secret agent listening in for revealing clues. It is also the opposite of the camera, the extended CCTV-surveillance that appears to pry into the intimate and intricate details of everyday life. The content/metadata distinction therefore justifies the practices of intelligence agencies, as ultimately they are deemed to be using a qualitatively different form of data.

Yet, this benign reading of metadata has been challenged by critics, who have argued, on the one hand,

that metadata is data about content and that the uses of metadata were no more devoid of knowledge than data is, on the other. For instance, Edward Snowden has pointed out that '[m]etadata is what allows an actual enumerated understanding, a precise record of all the private activities in all of our lives' (Plume, 2014). In an *Amici curiae* brief for the *ACLU v Clapper* case in the USA, filed by a coalition of non-governmental organizations (NGOs) in the wake of the Snowden revelations, several computer scientists have emphasized the sensitivity of metadata in similar terms and challenged the hierarchy that President Obama and the intelligence experts set in place. 'The pool of telephony metadata collected by the government', they note, 'reveals a wealth of deeply personal and intimate information about millions of Americans' (Abelson et al., 2014). These critics draw attention to the relationships between (telephony) metadata, content, and information. Networks of people can coalesce around certain phone numbers of, for instance, their local sports centre. Thus, telephony metadata oozes with meaning, which makes its distinction from content problematic.

Indeed, this distinction between metadata and content has been contested by critical scholars and civil liberties activists alongside whistle-blowers and computer scientists. However, we contend that there are limitations to the critical arguments that metadata = data = knowledge. In information science, the field of knowledge engineering covers the transformation of content into data that computers can process. For knowledge engineering, content is really anything that can be expressed digitally like any video, software, text, or audio. In our case, content is, for instance, a phone conversation. Knowledge engineering sets out to discover all computer-actionable data in this content. Communications (meta)data such as location and time is an important part of this data. Computers prefer (meta)data to content, as the former is structured and semantically defined for their processing. The distinction between content and (meta)data, which is invoked and justified by the professionals of security and politics, relies on an implicit hierarchy of knowledge production that underlies the field of knowledge engineering. In computing and information science, this hierarchy is generally referred to as data-information-knowledge (DIK) and is widely discussed as one of the foundational issues of these disciplines. The taxonomy of data-information-knowledge starts with 'raw' data and systematically builds information and finally knowledge.

For the purposes of our argument, what counts is the fact that professionals of security and politics relegate (meta)data to the bottom of the supposed DIK hierarchy. This has important implications, as it might mean that the collection of data in all its forms is regarded as irrelevant and 'encourages the mindless and meaningless collection of data in the hope that one day it will ascend to information – pre-emptive acquisition' (Frické, 2009: 136). In this sense, the DIK hierarchy enables Obama and others to claim that the bulk collection of metadata is not politically significant and only becomes problematic once it has been transformed into information and knowledge. Data becomes a raw and neutral material ready to be mined.

As the hierarchy of DIK is translated into the political realm, security professionals take up what is an essentially messy distinction from computer and information science and transform it into an absolute one in order to justify knowledge production about 'known and unknown terrorists'. In a declassified opinion from the US Foreign Intelligence Surveillance Court (FISC) in the wake of the Snowden revelations, Judge Claire Eagen noted that 'it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives . . .' (FISC, 2013: 18).

To avoid this move to the irrelevance of (meta)data, computer and information scholars have challenged the strict separation of categories and the DIK hierarchy. This move is not quite the same as the recent re-evaluation and claim by critical scholars that 'there is no such thing as raw data' (Gitelman, 2013; Lyon, 2014) or that data is not simply 'pre-analytical and pre-semantic' (Markham, 2013). Information scientists have indeed long argued that the imagination of data as 'discrete objects that can be located in time and space' or as 'raw numbers and facts' (Alavi and Leidner, 2001: 109) is fundamentally flawed. Ilkka Tuomi goes furthest by stating that 'data is more than knowledge' (1999). Yet, they have also emphasized that data needs to be understood in the context of more fluid boundaries between data, information and knowledge (Alavi and Leidner, 2001; Frické, 2009; Tuomi, 1999). In the *Amici curiae* mentioned supra, computer scientists have pointed out that:

> Although the law may try to draw hard and fast distinctions between the two, see, e.g., Smith v. Maryland, 442 U.S. 735, 741 (1979), the reality is far murkier and typically depends on context. A change in technical protocols or standards can cause information traditionally regarded as metadata to be treated as content, and vice-versa. *But the task here is not to define ''metadata,'' nor do amici believe it practical or useful to do so in a categorical way*. (Abelson et al., 2014, emphasis ours)

While the interpretation of metadata as yielding information about individuals has ultimately come to be accepted by the US Court of Appeals of the Second Circuit in its judgement in *ACLU v Clapper*, the Court's interpretation of metadata remains beholden to a question of privacy (ACLU v Clapper, 2015: 10) and does not take up the computer scientists' argument about the problematic boundaries between kinds of data.

Data and metadata both refer to particular practices of knowledge production in the context of the field of knowledge engineering, which simultaneously draw boundaries (often through standards) between structured/unstructured data, information and knowledge. These distinctions are compounded by political distinctions between kinds of data and metadata. The UK Parliament's Intelligence and Security Committee recent report on security and privacy recognises these fluid epistemic and political boundaries:

> Metadata is a term commonly used in the USA, but it has no legal definition in the RIPA and therefore no bearing on the UK system of interception. For example, in the UK a record of a website visited (e.g. http://www.google.com) is treated as CD [communications data], whereas the full web address, which includes the precise words searched (e.g. http://www.google.co.uk/search?q=ISC), is treated as content. (Intelligence and Security Committee, 2015: 52)

The critical move is not to ask for clarity and definitions more adapted to digital technologies, as many NGOs and legal scholars suggest.[2] It is also not sufficient to subsume these to an overarching concept of knowledge. Translating concepts of knowledge from social science to this debate risks reproducing a similar dis-counting of data. It also risks downplaying the processes of (meta)data production. (Meta)data is not simply a question of interpretation by analysts (Bauman et al., 2014) or of data always being 'cooked'. (Meta)data can simply be technical, like the time and place of a particular phone call, and still be meaningful.[3]

The turn to metadata in the emerging Big Data-security assemblage needs to be understood in the context of an economy of Big Data production where 'digital sources create data as a by-product' (Ruppert et al., 2013) and we become 'walking data generators' (McAfee and Brynjolfsson, 2012). Data itself is a complex epistemic object, and distinctions between kinds of data are produced depending on how data is actionable by digital devices. In another *Amici curiae* submitted by the Electronic Frontier Foundation and ACLU in another legal case, *Klayman v Obama,* we are reminded that 'structured data, including telephony metadata, is ideally suited for computational analysis' (EFF and ACLU, 2014: 11). Thus, theories of (meta)data production and the critique of the DIK hierarchy are important moves that challenge the justificatory discourses of security professionals. At the same time, the problematization of metadata in the emerging Big Data-security assemblage needs to be supplemented by the understanding of how kinds of data are produced as actionable by digital devices. It is structured data that is an essential component in the work of Big Data organizations (Ekbia et al., 2015). A critique of NSA and GCHQ surveillance practices entails taking seriously the production of data as a heterogeneous epistemic and political object. 'Making up people' (Hacking, 1999) needs to be supplemented today by 'making up data'.

Seeing like a computer? Big Data as artificial intelligence

A second argument in the controversies about digital surveillance has been formulated in terms of controlled entries to and views onto data. Critics have drawn attention to the practices of 'mass surveillance' and their effects on human rights and democracy (Bauman et al., 2014; De Hert and Gutwirth, 2006; Rouvroy and Poullet, 2009). Security professionals have attempted to justify these practices as non-intrusive by arguing that it is computers that read data first and foremost, while humans only see little of what is otherwise processed by machines. Justificatory discourses of 'bulk data collection' and targeted rather than mass surveillance have hinged upon a distinction between humans and machines, computers and analysts. In an op-ed for the *New York Times,* Charles A Shanor, a professor of law, asks:

> shouldn't I be concerned that F.B.I. agents are trampling my rights, just like the I.R.S. might have trampled the rights of certain organizations seeking tax-exempt status? As it turns out, the answer is no. The raw 'metadata' requested will not be directly seen by any F.B.I. agent. (2013)

He goes on to argue that it is in fact a computer that sorts 'through the millions of calls and isolates a very small number for further scrutiny' (Shanor, 2013) and finds it a better option than the transparency advocated by human rights activists. In the *ACLU v Clapper* case mentioned earlier, Judge William Pauley III based his decision to dismiss the case on similar arguments put forth by Theresa Shea, Director of Signals Intelligence Directorate at NSA, that '*only a very small percentage of the total data collected is ever reviewed by intelligence analysts'* (2013). Shea explicates that '[a]lthough bulk

metadata are consolidated and preserved by the NSA pursuant to Section 215, *the vast majority of that information is never seen by any person*' (2013: 8, emphasis ours).

Shea and other intelligence experts invoke an analogy between NSA bulk data processing and targeted surveillance. Ultimately, the assumption is that there is no surveillance where data in not 'seen' by a human being. The human/machine distinction, with humans supposedly only coming in at the end of the data processing, aims to render these practices of data collection and processing legitimate by enacting a strong separation between humans and machines. These justifications do not only deactivate criticisms about mass surveillance, but are mobilized to disable claims before the law. James R Clapper, the Director of US National Intelligence, pursues this strategy to ask for a dismissal in *ACLU v Clapper*: 'those injuries could arise only if metadata associated with plaintiffs' calls were actually reviewed by a person, and plaintiffs do not dispute that only a small fraction of the Section 215 telephony metadata is actually reviewed by any person' (Clapper et al., 2014).

In the UK, the 2013 Annual Report of the Interception of Communications Commissioner reiterates this logic, where GCHQ data mining is deemed legal given that 'intrusion in this context into the privacy of innocent persons would require *sentient examination* of individuals' communications' (May, 2014, emphasis ours). In the UK Parliament's recent public inquiry on security and privacy, the reasoning follows the same strong binary of human/machine, as the report concludes that only 'a tiny fraction' of collected data is 'ever seen by human eyes' (Intelligence and Security Committee, 2015).

The justification of the separation between humans and computers is difficult to sustain if we understand the computing involved in terms of socio-technical assemblages, an unstable and contingent collection of heterogeneous elements (Latour, 2005). Yet, this distinction has been much more resistant to critique than the metadata/data distinction. To push our critical vocabularies further, it is not enough to point out that the Big Data-security assemblage is socio-technical. We need to understand not just human–non-human relationality, but also 'the content of the relationships that hold assemblages in place' (Allen, 2011: 156). What matters in the Big Data-security assemblage is how the relation between humans and computers gains content, and how the assembling of humans and computers is both an association and a division of labour.

Big Data organizations are characterized by a new division of labour between humans and computers (Blanke, 2014; Brynjolfsson and McAfee, 2011) that is about integrating human and machine reasoning at each step of processing relevance and learning how to distinguish significant and non-significant information from each other. In this division of labour, humans and machines are brought together in the same infrastructures to process the data. Recent advances in information systems have focused on connections between humans and computers, given a fundamental shift in how these systems are designed as artificial intelligence applications. A historical perspective on information systems for artificial intelligence helps shed light on this division of labour.

In social sciences, debates about automation, robotics, and data-driven science also suggest a change in human/non-human assemblages. Much critical work has focused on a shift towards computational decision-making and has downplayed the division of labour between humans and computers. We propose a different reading of human–computer assemblages by revisiting historical debates and transformations in the wake of the so-called 'winter of artificial intelligence' (AI). The phrase captures the perceived failure in the late 1980s of attempts to develop analytical capacities that would bring computing machines close to human intelligence. All the enthusiasm and the early promises of creating the thinking machines seemed gone. However, theoretical and practical breakthroughs in artificial intelligence capacities have since put in doubt this supposed 'winter' (Kurzweil, 2005: 264), as AI has developed a new type of 'intelligence' by combining human and computer reasoning.

In a reply to Noam Chomsky's critique of artificial intelligence, Peter Norvig (2012), Google's Director of Research, captures the epistemic transformation that took place in the 1980s. The 'winter of AI' was related to an over-reliance on logical models to simulate human reasoning and their subsequent failure. Computing scientists wanted to create an artificial intelligence that replicated human intelligence, but was separate from humans. Norvig (2012) locates an epistemico-material transformation from logical models to statistical models which 'have achieved a dominant (although not exclusive) position.' Unlike logical models, statistical models focus on assemblages of humans and machines that can process data. Rather than re-creating a black box that veils how humans reason, artificial intelligence has focused on building models that can solve particular problems. These models are developed within complex workflows of human–computer interaction, starting with large testbeds to tune algorithms so that they simulate human judgement on information relevance or expressed sentiments. In order to perform, algorithms need to be constantly evaluated for their effectiveness.

The epistemic crisis of AI has led to a reconfiguration and integration of human work and intelligence

into new human–computer assemblages. Information systems to develop analytical capacities have thus been built in a similar way since the winter of AI. Security systems in all their components share with other data science applications that they are also the result of the winter of AI, when research and funding shifted from 'wild-eyed dreams' of creating a human-like machine and started to concentrate on particular applications that were made possible by fostering different connections and division of labour between humans and computers.

In these models, humans do not interact with the data just at the end, but are involved at every stage through evaluation, optimization, training, etc. Yet, this does not mean that computers are simply passive tools, because as much processing as possible needs to be computerized. Computers should learn 'unsupervised' or, to put it differently, develop agency in these assemblages. A successful unsupervised learning technique is, for instance, the so-called topic modelling, which auto-summarizes a collection of documents into a number of common topics. In security applications, for instance, topic modelling is used to summarize cyber-threats in web data mining. However, these topic models can be too suggestive and require careful intervention by humans (Schmidt, 2011). Even so-called 'unsupervised' techniques are not black boxes but a human–computer assemblage.

Similarly, since 2006 we have witnessed yet another transformation in machine learning techniques through 'deep learning' for speech and image recognition. Again, however, as soon as one analyses the components of this new black box, it becomes apparent that even deep learning as the state-of-the-art in unsupervised computational learning requires human participation. Rather than becoming autonomous, computers are still enrolled in a socio-technical assemblage. Two leading machine-learning researchers, Socher and Manning, thus define machine learning as the 'numerical optimization of weights for human-designed representations and features' (2013). Security analytics is no different from other domains that enrol computers, artificial intelligence practices and data scientists.

In analysing this emerging assemblage through the transformation of AI, we have built upon critical work that draws attention to the socio-technical character of Big Data (Lyon, 2014). Yet, our analysis also shows how relations in a socio-technical assemblage gain content historically. Debates in AI have reconfigured the human–computer assemblage through an epistemico-material division of labour between humans and computers. This re-reading of Big Data through the history of AI also allows us to challenge the credibility of the distinctions that security professionals attempt to institute between computer-based targeted surveillance and mass surveillance by showing how the 'winter of AI' has led to particular modes of assembling computers, techniques of machine learning and (data and security) analysts.

Algorithmic security: Anticipation and probabilities

A third and related site of controversy in the emerging Big Data-security assemblage has focused on the epistemic capabilities of algorithms. Intelligence experts speak about these capacities as finding the 'needle in a haystack' and the NSA's General Alexander as 'connecting the dots'. In an intervention before the US Congress following the Snowden revelations, former Federal Bureau of Investigation (FBI) Director Robert Mueller noted that 'If you narrow [the scope of surveillance], you narrow the dots and that might be the dot that prevents the next Boston' (Roberts, 2013). The shift in reasoning towards the anticipation of possibilities, conjecture and speculation underpins the justifications that security professionals proffer for the necessity of extensive Big Data mining. Critical security and surveillance scholars have analysed the recalibration of security practices through anticipatory knowledge (Amoore, 2014; Aradau and van Munster, 2011; Cooper, 2008; de Goede, 2012; Lyon, 2014). Critical data studies have highlighted to the predictive fallacy of Big Data, the tension between correlation and causation, the 'return to empiricism', and the opacity of algorithms (Boyd and Crawford, 2012; Ekbia et al., 2015, Kitchin, 2014; van Dijck, 2014).

As important as these criticisms are, they do not address the perceived necessity to 'collect it all', the whole 'haystack' of data, in order to enhance the capabilities of algorithms. As Judge Pauley III glosses in *ACLU v Clapper*, the bulk metadata collection programme is 'a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data' (ACLU v Clapper, 2015). Security professionals talk about 'needles in haystacks' and take the necessity of collecting and creating an ever-larger 'haystack' of data for granted. Thus, the fact that all the data is needed for the purposes of terrorism prevention becomes unquestionable:

> No doubt, the bulk telephony metadata collection program vacuums up information about virtually every telephone call to, from, or within the United States. That is by design, as it allows the NSA to detect relationships *so attenuated and ephemeral they would otherwise escape notice*. (ACLU v Clapper, 2013: 52, emphasis ours)

These statements become meaningful through the promise of algorithms to unveil the 'unknown

terrorists' through the anomalous clues and features that cannot be easily clustered and do not fall under a normal pattern.[4] Algorithms appear to institute the new: new processes, rationalities, and techniques of decision-making. Critical discussions about algorithms and algorithmic reasoning have focused on the 'ontology of association' (Amoore, 2011) and the secret nature of the algorithms used by intelligence agencies and businesses (Pasquale, 2015). We argue that critical discourses need to engage more closely with algorithmic practices. Here, we focus on two elements of algorithmic practices: the relation between data and algorithms, and probabilistic methods.

Firstly, we take seriously Norvig's widely quoted claim that Google does not necessarily have better algorithms than everybody else, but more data (quoted in Schutt and O'Neil, 2013). Marissa Mayer, Google's former VP of Search Products and User Experience, had also noted 'that having access to large amounts of data is in many instances more important than creating great algorithms' (quoted in Perez, 2007). Data has become more important than algorithms themselves, because '[t]here is no single scientific breakthrough behind Big Data. On the contrary, the methods used have been well known and established for quite some time' (Lehikoinen and Koistinen, 2014: 39). Secondly, we analyse algorithms through the probabilistic methods that all algorithms deploy independent of their exact design in particular institutions. Discourses of the 'novelty' of Big Data and algorithmic capacities need to be located within probabilitistic methods and their limitations, which are the foundation of Big Data analytics as they allow reasoning about uncertainty (Bengio et al., in preparation).

Justificatory discourses of the capabilities of Big Data for security governance activate a particular imagination of the relation between part and whole. The haystack metaphor that security professionals are using is no longer a metaphor for a sample size but for Big Data, where '$N = $ all' (Mayer-Schönberger and Cukier, 2013). All data appears now to be needed or, in a formula repeated by Big Data enthusiasts, data is 'unreasonably effective' (Halevy et al., 2009). This not only drives Big Data to become even bigger but it also motivates engineers to trust probabilistic reasoning as a way to render uncertainty mathematically (Frické, 2014: 3).

Shifting from the focus on algorithms to the data that algorithms need and the modes of probabilistic reasoning designed for algorithmic processes allows us to develop a critical vocabulary about the 'needle in a haystack'. Security professionals have justified this need for an infinitely expanding haystack through the idea that having all the data can algorithmically reveal better knowledge about potential terrorists, which would make pre-emptive action possible. However, this imaginary of Big Data that yields better knowledge has been challenged in debates about Big Data. Bigger data is not better 'without limit' (Frické, 2014: 5).

Let us take an example, which has been at the heart of claims about the unreasonable effectiveness of data: Google. Google engineers can rely on the 'unreasonable effectiveness' of web page data, because these pages consist of words whose meaning can be derived from the frequencies with which these words appear within web pages. Over time, 'human language has already evolved words for the important concepts' (Halevy et al., 2009: 12). Security applications, on the other hand, share with Big Data applications in humanities and social sciences the interest in shifting concepts and 'minority' vocabularies, rare words and rare data. While standard algorithmic reasoning can be 'successful for a lot of things' that follow regularities, 'it amounts to a deliberate neglect of rare words' (White, 2011). Statistical algorithms tend to ignore rare data, especially as the models get more complex in social domains and are tightly fitted to their original training data. In the language of machine learning for Big Data, these models are 'overfitted' to the training data and are challenged by new unknown data items. According to the data scientist Janert (2010: 424), the 'nature of statistical learning' requires us to add more and more dimensions to our data and move further away from the rare variables.

Another example of the fallacy to 'collect it all' for the purposes of data analytics is the analysis by the computer scientist and outspoken critic of NSA data mining Edward Felten (2014), where he shows how in typical data reasoning reduced data sets can lead to better results than large data sets. He argues that if the NSA covers larger numbers of phone connection hops, starting from a phone number they have under surveillance, this will not render the security analytics more effective. As Felten shows using typical algorithms, the fewer the hops involved (i.e. the smaller the sample), the better the results. The NSA drive to collect and mine Big Data understood as 'all data' is revealed as a myth.

The drive to collect more and more data is not just based on a Big Data myth but can be counterproductive not just for the fitting of the machine learning algorithms but also for their methods, as it generally leads to many false positives. Computer scientists involved in mining Big Data have argued for a long time that the larger the haystack, the more likely it is that only meaningless events are added. A comparison of random and non-random events will lead to an overestimation of the non-random ones. One of the standard textbook introductions to machine learning makes an important point for our discussion (Leskovec et al., 2011). In

offering a standard example of predictive data analytics for counter-terrorism, the authors develop a criticism of the assumption that if the haystack is just big enough and enough data is collected, the ocean of data will automatically also increase the possibilities to find the needle in the data.

Starting with a typical data mining case for counter-terrorism, Leskovec et al. (2011) work with the assumption that two people are considered to be suspicious if they stayed more than once in the same hotel at the same time, which is a typical assumption in security analytics. In their example, if one billion people were to be tracked over a period of 1000 days, there will be a well-defined probability that two random people stay at the same hotel more than once. This probability is quite small and might therefore look promising for identifying potential suspects. The problem is, however, that in these millions of people there are many possible pairs of people who could have stayed at the same hotel. In their calculation, the result was over 250,000 of such 'suspicious' pairs (Leskovec et al., 2011). Therefore, as computer scientists know, the error in data mining methods actually rises if more and more data is collected, which is contrary to the belief that an 'ocean of data' makes it possible to identify 'gossamer contacts' with more certainty.

The production of large numbers of false positives in the 'ocean of data' raises another question for Big Data mining – how to distinguish 'real' and 'false' suspects. According to Felten (2014), rather than predicting new terrorist activities, typical NSA security analytics algorithms are designed for more realistic use cases in order to avoid overfitting and overestimation of false positives. These algorithms are designed to substantiate the suspicion a security analyst already has, rather than predict new suspects or suspect behaviour, as the analogy of the 'needle in a haystack' might suggest. These algorithms are thus not good at eliminating suspicion. In general, they do not help to find the needle in the haystack but help confirm whether there is reason to assume that there might be a needle. Big Data mining has never been good at evaluating false positives, which is less of an issue for an Internet search engine where users get used to skipping irrelevant results, but is an issue in a security context where innocent people become suspicious.

Contra the FBI director Robert Mueller's concern that a narrower focus of surveillance will miss the dots that need to be connected in order to prevent the 'next Boston' (Roberts, 2013), computer scientists have shown that it is often the wider focus that has this effect. If data grows big, both the apparent risk of a terrorist attack and the number of suspicious people will vastly increase. In terms of the theory of data mining, this problem can be seen as typical of distributions with heavy tails, which are those distributions that are extremely skewed with a long tail of events that happen sometimes but not very often.

The 'next terrorist attack' is a possible event of low probability such as the 'rare words' for which Google's data enthusiasm is less reasonably effective, as discussed supra. Security-relevant activities are generally heavy-tailed, as they are conducted by a small number of people compared to the overall population. The corresponding heavy-tailed distributions require special methods in order to apply algorithmic reasoning (Clauset et al., 2007). General statistical assumptions about what can be reasonably expected as the next event do not work, because these are 'distributions without expectations' (Janert, 2010: 201). The mean event, for instance, does not reveal anything about the expected behaviour of the distribution. For heavy-tailed distributions, events outside the tail do not indicate anything about events in the tail where the suspects can be found. Similarly, the random behaviour of those who are not suspicious does not tell us much about the behaviour of suspects and vice versa. Making the data 'big' will therefore not reveal anything that can be used to identify suspects, as long as we do not know whether this data belongs to the tail.

In order for data mining to work on heavy-tailed distributions, these are often split up into various subgroups where each of them is dealt with individually. To make these divisions, cut-off points need to be found that analysts consider as indicative of suspicious behaviour in the tail. For instance, all those are suspects who call the same phone number in Maryland. These features generally cannot be just read from the data, but an analyst needs to make a decision as to which features count to identify a suspect (Janert, 2010: 434). Big Data algorithms require specialized theories and domain assumptions like the feature that suspects call the same number in Maryland. Formally speaking, without assumptions about the data, Big Data mining algorithms do not perform better on new information than any random prediction; this is independent of the size of the data set (Wolpert and Macready, 1997).

The metaphor of finding the needle in the haystack is a powerful one used by Big Data professionals and then reused by security professionals, judges and politicians. While it seemingly justifies the huge effort of collecting more and more data in order to cover all possibilities, the metaphor effaces debates in computer science about the epistemic limits of algorithmic practices and methods. Developing a critique of anticipatory algorithmic security entails an immanent critique of algorithmic practices and methods.

Conclusion: Theses on critique

On 7 May 2015, the US Court of Appeals for the Second Circuit overturned the decision in *ACLU v Clapper* that granted the government's motion to dismiss and argued that the programme was unlawful under §215 of the Patriot Act (2015). The decision draws on the declaration by Edward Felten and other *Amici curiae* information, which have disputed the government's justification of telephone (meta)data collection. While the Court does not address the challenge of constitutionality, the decision highlights the importance of computing knowledge to challenge the credibility of claims made by security professionals. At the same time, the judges have left a series of other assumptions about surveillance by computers and the algorithmic capabilities unquestioned.

In order to address the impasses of critique in public and academic controversies, this paper has proposed a series of reformulations of existing critical vocabularies of the Big Data-security assemblage. A collaboration between social sciences, and computer and information sciences, as developed here, can challenge the credibility of the justifications promoted by intelligence agencies such as the NSA and the GCHQ and contribute to research agendas in critical approaches to security and surveillance, on the one hand, and critical data studies, on the other. Rather than assuming that informatics is 'the discipline of choice of liberal power' (Bauman et al., 2014, 139), we have interpreted a series of debates in knowledge engineering, artificial intelligence and data mining in order to address the limits and impasses of critical engagements with Big Data in security governance. Methodologically, we have been able to eschew the invocation of secrecy around NSA and GCHQ practices by engaging with the state-of-the-art in computer and information sciences. As employers of computer scientists, mathematicians, and physicists, we have contended that the NSA and the GCHQ are unlikely to have developed technologies and methods beyond the latest research in academic and commercial organizations. Yet, despite the apparent credibility of their discourses being grounded in the scientificity of these disciplines, we have shown that debates in computer and information science challenge this credibility. We have combined this engagement with computer and information science with an analysis of legal cases, public inquiries, parliamentary and media reports, and declassified documents in the wake of the Snowden revelations.

We have developed a two-pronged argument. On the one hand, we have shown that the invocations of privacy, mass surveillance and decisions by algorithms run into political and epistemic impasses as they have been continually challenged by professionals of security and politics. On the other, we have argued for different vocabularies of critical intervention in the sites of controversy in the emerging Big Data-security assemblage: from metadata privacy to the production of data as a complex epistemic entity; from mass surveillance by computers to the division of labour between humans and computers in artificial intelligence; from an underlying algorithmic logic of security to algorithmic practices and probabilistic methods. These interventions suggest several trajectories for developing critical research about data in security governance. By way of conclusion we propose four theses on critique:

Thesis 1

Big Data theories and methods are not as new or revolutionary as the justificatory discourses of security professionals and many critical academic analyses of Big Data suggest. Rather than assuming a 'Big Data revolution', the deployment of Big Data for security purposes needs to be understood in terms of what Michel Foucault has called the 'inflection of the curve' (1998 [1976]).

Thesis 2

Data is a complex epistemic object. Therefore, data needs to be approached as an object of inquiry rather than subsumed to knowledge. Meanings of data, metadata, and knowledge differ between social sciences and information science. Rather than simply contending that there is no such thing as raw data, critical data studies need to analyse the 'making up' of data and the production of kinds of data at the juncture between information and computer science, on the one hand, and politics, on the other.

Thesis 3

The digital age does not mean that decisions are simply transferred from humans to computers and algorithms. We are only beginning to understand the transformation of intelligence agencies (and other security organizations) into Big Data organizations. There is little existing work on the details of this organizational change, which entails understanding histories of Big Data as artificial intelligence, and particularly the reconceptualization of the relation between humans and computers in AI. Analyses of data-security assemblages need to attend not just to the modes of association and heterogeneous elements of an assemblage, but equally to how it gains content through a division of labour between humans and computers.

Thesis 4

There are no 'unreasonably effective' algorithms. Critical approaches to security and surveillance need to engage with the methods and routine practices of Big Data-security analytics. Algorithms continue to rely on probabilistic methods, which depend on and are challenged by the increased amounts of data produced today. Unless we analyse the algorithmic practices and methods from information and computing sciences, we might write and critique only the science fiction of security analytics.

Declaration of conflicting interest

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

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. For critical engagements, which challenge the relevance of liberal concepts of privacy and human rights for the digital age, see for instance Finn Brunton and Nissenbaum (2011).
2. See the International Principles on the Application of Human Rights to Communications Surveillance, a global consultation on a framework to evaluate digital surveillance practices (https://en.necessaryandproportionate.org/text).
3. Although for reasons of space we cannot discuss the various kinds of metadata, we should mention here that in information science there is a distinction between administrative and technical metadata as well as descriptive metadata. The latter are, for instance, keywords that describe the content of a phone call, while the former are, e.g., timestamps of phone calls. All these types of metadata are used in surveillance and the boundaries between them are fluid (Miller, 2011). Especially technical metadata such as timestamps is easily structured data in the processing pipelines of knowledge engineering.
4. The lack of evidence of a high number of thwarted terrorist plots by the NSA and the GCHQ did not undermine the argument that having the whole haystack could potentially predict the 'next terrorist attack'.

References

Abelson H, Appel AW, Bellovin SM, et al. (2014) *Amici curiae brief of experts in computer and data science in support of appellants and reversal*, 3 March. Available at: https://www.eff.org/files/2014/03/13/clapper_amicus_-computer_scientists.pdf (accessed 20 July 2015).

ACLU v Clapper (2013) 13 Civ. 3994 US SDNY (27 December 2013). Available at: http://www.nysd.uscourts.gov/cases/show.php?db=special&id=364 (accessed 20 November 2014).

ACLU v Clapper (2015) N0 14-42 US Court of Appeals for the Second Circuit (7 May 2015). Available at: http://www.ca2.uscourts.gov/decisions/isysquery/773a98db-d41d-4db8-95aa-182f994923b5/1/doc/14-42_complete_opn.pdf (accessed 7 May 2015).

Alavi M and Leidner DE (2001) Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly* 25(1): 107–136.

Allen J (2011) Powerful assemblages? *Area* 43(2): 154–157.

Amoore L (2011) Data derivatives. *Theory, Culture & Society* 28(6): 24–43.

Amoore L (2014) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.

Amoore L and de Goede M (2005) Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change* 43: 149–173.

Aradau C and van Munster R (2011) *Politics of Catastrophe: Genealogies of the Unknown*. Abingdon: Routledge.

Bauman Z, Bigo D, Esteves P, et al. (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121–144.

Bengio Y, Goodfellow IJ and Courville A (in preparation) Deep learning. Available at: http://www.iro.umontreal.ca/~bengioy/dlbook (accessed 24 April 2015).

Bigo D (2008) Globalized (in)security: The field and the banopticon. In: Bigo D and Tsoukala A (eds) *Terror, Insecurity and Liberty: Illiberal practices of liberal states after 9/11*, Abingdon: Routledge, pp. 10–49.

Blanke T (2014) *Digital Asset Ecosystems: Rethinking Crowds and Clouds*. Oxford: Chandos/Elsevier.

Bonditti P (2008) Homeland security through traceability. In: Dunn Cavelty M and Soby-Kristensen K (eds) *Securing 'the Homeland': Critical Infrastructure, Risk and (in) Security*. Abingdon: Routledge, pp. 130–152.

Boyd D and Crawford K (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662–679.

Brunton F and Nissenbaum H (2011) Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday* 16(5). Available at: http://firstmonday.org/article/view/3493/2955 (accessed 29 September 2015).

Brynjolfsson E and McAfee A (2011) *Race Against the Machine*. Lexington: Digital Frontier Press.

Clapper JR, et al. (2014) Brief for defendants – Appellees. In: *Docket No 14-42*. United States Court of Appeals for the Second Circuit.

Clauset A, Young M and Gleditsch KS (2007) On the frequency of severe terrorist events. *Journal of Conflict Resolution* 51(1): 58–87.

Cooper M (2008) *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*. Seattle, WA: University of Washington Press.

De Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.

De Hert P and Gutwirth S (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: Claes E, Duff A and Gutwirth S (eds) *Privacy and the Criminal Law*. Antwerpen: Intersentia, pp. 61–104.

EFF and ACLU (2014) *Amici Curiae*. The United States Court of Appeal for the District of Columbia Circuit 2014. Available at: https://www.eff.org/en-gb/document/eff-and-aclu-amicus-brief-klayman (accessed 4 April 2015).

Ekbia H, Mattioli M, Kouper I, et al. (2015) Big data, bigger dilemmas: A critical review. *Journal of the Association for Information Science and Technology* 66(8): 1523–1545.

Felten E (2014) Technical Tradeoffs in NSA's Mass Phonecall Data Program 2014. Available at: https://www.youtube.com/watch?v=tyPL_sN776k (accessed 3 June 2014).

FISC (2013) Re application of the federal bureau of investigation. *BR 13-109*. Washington, DC: US Foreign Intelligence Surveillance Court (FISC). Available at: https://www.aclu.org/files/assets/br13-09-primary-order.pdf (accessed 28 September 2015).

Foucault M (1998 [1976]) *The History of Sexuality I. The Will to Knowledge*. 3 vols. London: Penguin Books.

Frické M (2009) The knowledge pyramid: A critique of the DIKW hierarchy. *Journal of Information Science* 35(2): 131–142.

Frické M (2014) Big data and its epistemology. *Journal of the Association for Information Science and Technology* 66(4): 651–661.

Gitelman L (2013) *Raw Data is an Oxymoron*. Cambridge, MA: MIT Press.

Hacking I (1999) Making up people. In: Biagioli M (ed.) *The Science Studies Reader*. New York: Routledge, pp. 161–171.

Halevy A, Norvig P and Pereira F (2009) The unreasonable effectiveness of data. *Intelligent Systems, IEEE* 24(2): 8–12.

Hildebrandt M (2013) Slaves to big data. Or are we? *IDP. Revista de Internet, Derecho y Politica* (17). Available at: http://journals.uoc.edu/index.php/idp/article/viewFile/n17-hildebrandt/n17-hildebrandt-en (accessed 24 April 2015).

Intelligence and Security Committee (2015) *Privacy and Security: A Modern and Transparent Legal Framework*. House of Commons. Available at: http://isc.independent.gov.uk/committee-reports/special-reports (accessed 12 March 2015).

Janert PK (2010) *Data Analysis with Open Source Tools*. Cambridge, MA: O'Reilly Media.

Kitchin R (2014) Big data, new epistemologies and paradigm shifts. *Big Data & Society* 1(1): 1–12.

Kurzweil R (2005) *The Singularity is Near*. New York, NY: Viking.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-network-theory*. Oxford: Oxford University Press.

Lehikoinen J and Koistinen V (2014) In big data we trust? *Interactions* 21(5): 38–41.

Leskovec J, Rajaraman A and Ullman JD (2011) *Mining of Massive Datasets*. Cambridge: Cambridge University Press.

Lyon D (2014) Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society* 1(2). DOI: 10.1177/2053951714541861.

Markham AN (2013) Undermining 'data': A critical examination of a core term in scientific inquiry. *First Monday* 18(10). Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/4868/3749 (accessed 29 September 2015).

May A (2014) *2013 annual report by the interception of communications commissioner*. London: Interception of Communication Commissioner's Office.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution that will Transform how We Live, Work, and Think*. London: John Murray.

McAfee A and Brynjolfsson E (2012) Big data: The management revolution. *Harvard Business Review* 90: 60–69.

Miller SJ (2011) *Metadata for Digital Collections: A How-to-do-it Manual*. New York, NY: Neal-Schuman Publishers.

Norvig P (2012) Colorless green ideas learn furiously: Chomsky and the two cultures of statistical learning. *Significance* 9(4): 30–33.

Obama B (2013) *Transcript: Obama's remarks on NSA Controversy* (7 June 2013). *The Wall Street Journal*. Available at: http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/ (accessed 2 July 2014).

Pasquale F (2015) *The Black Box Society*. Vol. 36. Cambridge, MA: Harvard University Press.

Perez J (2007) *Google wants Your Phonemes*. Available at: http://www.infoworld.com/t/data-management/google-wants-your-phonemes-539 (accessed 1 October 2012).

Plume K (2014) *Snowden, Greenwald Urge Caution of Wider Government Monitoring at Amnesty Event* (5 April 2014). *Reuters*. Available at: http://www.reuters.com/article/2014/04/06/us-usa-security-snowden-idUSBREA3500320140406 (accessed 12 May 2014).

Raley R (2013) Dataveillance and countervailance. In: Gitelman L (ed.) *''Raw data'' is an Oxymoron*. Cambridge, MA: MIT Press, pp. 12–146.

Roberts D (2013) FBI Chief Mueller says spy tactics could have stopped 9/11 attacks. *The Guardian*, 13 June.

Rouvroy A (2012) The end(s) of critique: Data-behaviourism vs. Due-process. In: Hildebrandt M and de Vries K (eds) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. London: Routledge, pp. 143–168.

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?* New York, NY: Springer, pp. 45–76.

Ruppert E, Law J and Savage M (2013) Reassembling social science methods: The challenge of digital devices. *Theory, Culture & Society* 30(4): 22–46.

Schmidt B (2011) Compare and contrast. In: *Sapping Attention. Digital Humanities: Using tools from the 1990s to answer questions from the 1960s about 19th century America*. Available at: http://

sappingattention.blogspot.co.uk/2011/11/compare-and-contrast.html (accessed 27 April 2015).

Schutt R and O'Neil C (2013) *Doing Data Science: Straight Talk from the Frontline*. Sebastopol, CA: O'Reilly Media, Inc.

Shanor CA (2013) Making a mountain out of a digital molehill. *New York Times*, 7 June. Available at: http://www.nytimes.com/2013/06/07/opinion/making-a-mountain-out-of-a-digital-molehill.html?_r=0 (accessed 28 September 2015).

Shea T (2013) Declaration of Teresa H Shea, Signals Intelligency Director, National Security Agency. In: *ACLU v Clapper 13 Civ. 3994 (WHP) ECF Case*: Southern District of New York.

Socher R and Manning C (2013) *Deep learning for natural language processing (without magic)*. Available at: http://nlp.stanford.edu/courses/NAACL2013/ (accessed 27 April 2015).

Tuomi I (1999) Data is more than knowledge: Implications of the reversed knowledge hierarchy for knowledge management and organizational memory. *Journal of Management Information Systems* 16(3): 107–121.

Van Dijck J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.

Weinberger D (2011) *Too Big to Know: Rethinking Knowledge Now that the Facts Aren't the Facts, Experts Are Everywhere, and the Smartest Person in the Room is the Room*. New York, NY: Basic Books.

Wheeler B (16 October 2014) Theresa May: We need to collect communications data 'haystack'. *BBC 2014*. Available at: http://www.bbc.co.uk/news/uk-politics-29642607 (accessed 19 January 2015).

White G (2011) Semantics, hermeneutics, statistics: Some reflections on the semantic web. Paper read at BCS-HCI '11 Proceedings of the 25th BCS Conference on Human–Computer Interaction, pp. 24–28.

Wolpert DH and Macready WG (1997) No free lunch theorems for optimization. *Evolutionary Computation, IEEE Transactions* 1(1): 67–82.