BIG DATA FOR SECURITY: A CULTURAL ANALYSIS

JANET CHAN AND LYRIA BENNETT MOSES

[2020] *UNSWLRS* 80

UNSW Law
UNSW Sydney NSW 2052 Australia

BIG DATA FOR SECURITY: A CULTURAL ANALYSIS

Janet Chan and Lyria Bennett Moses

UNSW Law (UNSW Australia, Sydney NSW 2052 Australia), and Data to Decisions Cooperative Research Centre

This is the original version of a paper (March 2016) that was revised and published as Chan J;Moses LB, 2017, 'Making sense of big data for security', British Journal of Criminology, vol. 57, pp. 299 - 319, http://dx.doi.org/10.1093/bjc/azw059.

BIG DATA FOR SECURITY: A CULTURAL ANALYSIS

Abstract

Big Data technology is said to hold great promise for improved efficiency and effectiveness for law enforcement and security intelligence agencies. This article aims to develop a cultural analysis of the potential impact of Big Data on the production of national and international security. Building on a Bourdesian framework for analysing police and new technologies, the article draws on empirical data from an Australian study to examine how security agents made sense of the capability and value of Big Data and developed technological frames that envisaged how this new technology could enhance or change their practices. The analysis demonstrates the importance of understanding the habitus of security agents in negotiating technological change in the field of security production.

Keywords

Big Data, Law enforcement, Security intelligence, Sensemaking, Technological frames, Cultural analysis

Manuscript

BIG DATA FOR SECURITY: A CULTURAL ANALYSIS

1. Introduction

'Big Data' is an amorphous concept that has been used to refer both to large, diverse, rapidly-changing datasets, or to the analytic techniques employed to extract information from such datasets. While some have attempted to refine the definition of 'Big Data' (see e.g. Kitchin 2014), others avoid the term, preferring 'data science' or 'data analytics'. Boyd and Crawford (2012: 663) take a broader view and describe 'Big Data' as 'a cultural, technological, and scholarly phenomenon' involving technology, analysis and mythology. The concept of 'Big Data' thus remains flexible, subject to the different interpretations among those who seek to analyse or employ data-related technologies for a wide variety of scholarly, commercial and government purposes (Bennett Moses and Chan 2014; Chan and Bennett Moses 2016).

It has been suggested that Big Data holds great promise for improving the efficiency and effectiveness of law enforcement and security intelligence agencies. For example, the Executive Office of the President (US) (Podesta *et al*. 2014: 29, 58) has claimed that '[b]ig data can be a powerful tool for law enforcement' and that it 'holds the potential to … substantially strengthen national security'. Similar claims about the use and potential of Big Data appear on websites and in other publications (see Wyllie 2013; Olesker 2012; Staniforth and Akhgar 2015).

This article aims to develop a cultural analysis of the potential impact of Big Data technology on law enforcement and security intelligence by conceptualising Big Data as a new *technique* of security that is being introduced into national and international security *projects* (Valverde 2014). Building on Chan's (2003) integration of Orlikowski and Gash's (1994) notion of *technological frames* into a Bourdieusian analysis of police's reception of new technologies, the article draws on empirical data from an Australian study to examine how security agents in law enforcement and national security agencies made sense of the capability and value of Big Data and developed technological frames that envisaged how this new technology could enhance or change their practices. The analysis demonstrates the importance of understanding the habitus of security agents in negotiating technological change in the field of security production.

The article is divided into nine parts. Part 2 develops a conceptual framework employed in our analysis. In particular, it integrates Valverde's (2014) 'security projects', Orlikowski and Gash's (1994) 'technological frames', Weick's (1995) 'sensemaking', and Bourdieu's theory of practice to explain how different social groups respond to the possibility of technological change. Part 3 summarises the findings of the available empirical research on the impact of technology on security practices. Part 4 briefly describes the research method and research participants. Part 5 analyses the working assumptions of security agents about current purposes of using data for security production. Part 6 describes security agents' framing of Big Data—its nature, capability and value—compared with other stakeholders. Part 7 explores their expectations about Big Data technology, while Part 8 examines their perceptions of the impact of Big Data on the distribution of capital in the field of security production. Part 9 concludes by summarising the findings and discussing their broader implications.

2. Making Sense of Big Data for Security

A useful starting point for analysing the potential impact of Big Data on security practice is to regard Big Data as an instance of 'technology'. Research in science and technology studies has concluded that 'technology' is not only a physical given (artefacts and technical systems), but also comprises knowledge about such systems as well as practices of handling them (MacKenzie and Wajcman 1985). Technology is constructed in the sense that it is 'made' and also in the sense that it is interpreted and understood through social groups influenced by a range of physical, social, political and organisational factors that may change over time (Bijker 2010). To understand how Big Data is constructed in the

context of law enforcement and security intelligence, it is useful, following Valverde (2014), to conceive of Big Data as a *technique* that is being introduced into one or more *security projects* in the governance of society. To set up a framework for examining the *logic* and *practices* of current Australian security projects, we build on the analytic tools used by Chan (2003) for understanding the impact of information technology on police practice. In particular, we use the notion of *technological frames* from science and technology studies and *sensemaking* from organisational studies and integrate them with concepts from Bourdieu's theory of practice. The development of this framework is explained below.

Security Projects

Valverde (2014: 382) has suggested that a fruitful way for researchers to study the governance of crime and security is to focus on security *projects*—'the governing networks and mechanisms that claim to be promoting security at all scales'. Instead of focusing on 'security' as a concept, she argues that we should look at the 'very wide variety of *activities* and *practices* that are being carried out under the name of "security"' (Valverde 2014: 383–4). In particular, it is important to examine the *logic*, spatiotemporal *scale*, *jurisdiction* and *techniques* of security projects. These aspects of security are more than what their labels suggest. For example, the notion of *logic* in this formulation goes further than the instrumental, rational dimension of governance to include its affective and aesthetic dimensions: 'the aims and the assumptions of a project – that which tells us what counts as relevant information – but also the culturally specific fears and moods that pervade the field of security' (Valverde 2014: 384). Similarly, *scale* has both spatial (or geographic) and temporal (both direction and duration) dimensions. A distinction identified by Valverde that is highly relevant to our discussion is that between past-focused exercises such as crime detection and criminal investigation and future-oriented activities such as crime prevention in the governance of security. *Jurisdiction* is not necessarily tied to geographical space but involves specifying 'the proper authority for space X or problem Y' and thus ends up determining how X or Y should be governed (Valverde 2014: 388). Finally, *techniques* of security encompass more than technologies or equipment; they can denote reporting formats, as well as law, architecture, bodily habits and other governance tools.

While Valverde's dimensions are useful for analysing security projects in general, concepts from science and technology studies and theories of practice can provide additional tools for examining the logic and practices in projects that involve technological change. The next section is devoted to a discussion of technological frames and sensemaking.

Technological Frames and Sensemaking

The notion of 'technological frames'[1] (Orlikowski and Gash 1994) is a useful tool for documenting how different social groups conceive of technology and respond to technological change. Drawing on the idea of frames in social cognitive research, Orlikowski and Gash (1994: 178) define the technological frame as 'that subset of members' organizational frames that concern the assumptions, expectations, and knowledge they use to understand technology in organizations'. While people hold individual interpretations about technology, members of a professional or occupational group may also have assumptions and beliefs that are shared within the group. Technological frames can be powerful in that they 'will strongly influence the choices made regarding the design and use of those technologies' (Orlikowski and Gash 1994: 179). Hence, the 'success' or otherwise of a technological change can be explained by the *congruence* or *incongruence* of technological frames between, for example, the architects and the users of a technology (Orlikowski and Gash 1994: 180).

In their own empirical research, Orlikowski and Gash (1994: 183–4) found three (overlapping) frame domains that characterise participants' interpretations of technology: (i) nature of technology, people's perception of the technology and its capabilities; (ii) technology strategy, people's views of the motivation behind their organisation's adoption of the technology and the value of this technology to the organisation; and (iii) technology in use, people's understanding of 'how the technology will be used on a day-to-day basis and the likely or actual conditions and consequences associated with such use'. The authors found incongruence in all three domains between the users and the technologists; these incongruences had led to unanticipated outcomes 'such as an initial barrier of skepticism and frustration and the perception that the office had not realized the benefits that were anticipated at the acquisition of [the technology]' (Orlikowski and Gash 1994: 198).

In assessing Orlikowski and Gash's (1994) contributions, Davidson (2006) suggests emphasising framing as a dynamic process involving 'interpretive power' and environmental triggers, and investigating the cultural and institutional foundations of technological frames. The idea of *sensemaking* (Weick 1995; Weick *et al.* 2005) is helpful in this regard. Technological frames are not static or frozen in time; they are formed as part of sensemaking—an ongoing process that people engage in to explicate the world and give it a sense of order. Technological change creates an 'occasion' for sensemaking. While people can draw on any information or cue to make sense of change, in practice they tend to draw on categories that summarise past experience such as cues found in traditions, standard procedures and assumptions that are salient in their group or organisation.

Davidson (2006) also sees important benefits for technological frames analysis to go beyond organisational boundaries, given that information technology increasingly requires the involvement of multiple organisations or whole industries. This is a particularly important point for understanding Big Data technology as it includes a conglomerate of techniques, modalities and applications that are applicable to myriad industries. In the next section, we propose broadening the technological frames concept to incorporate structure and the interplay between structure, sensemaking and frames.

Technological Change in the Field of Security Production

An integrated framework for understanding the potential impact of Big Data technology on law enforcement and security intelligence can be built from Chan's (2001, 2003) analysis of police responses to technological change. Chan (2003) draws on Bourdieu's notions of *field*, *capital* and *habitus* to focus on both structural and cultural determinants of social practice. Bourdieu's *field* is a 'social space of conflict and competition, where participants struggle to establish control over specific power and authority' (Chan 2003: 663). The field is often compared to a 'game' with different types of 'capital' (economic, cultural, social, symbolic) that are valued (Bourdieu 1987). Associated with each field is a system of dispositions (*habitus*) that agents in the field have acquired through family, education system or professional socialisation; it internalises the external structures and provides the dominant frame through which agents make sense of and act in the world. Habitus both 'sets structural limits for action' and 'generates perceptions, aspirations and practices that correspond to the structuring properties of earlier socialization' (Swartz 1997:101).

The field of security production is made up of various subfields, including (public or private) agents and agencies such as police and intelligence organisations concerned with maintaining order, preventing crime, enforcing laws or protecting lives and properties (cf McCahill's (2015) use of Bourdieu's theory to theorise the crime control field). Agents and agencies are differentiated not only in function, but also in power and resources. The logic of security projects (Valverde 2014)—their aims, assumptions, fears and moods—is manifest in the shared habitus of agents who operate in their (sub)field. Similarly, their technological frame (Orlikowski and Gash 1994)—the assumptions, expectations, and knowledge they use to understand technology—is a subset of agents' habitus.

For the purpose of this article, it is useful to conceive of the use of Big Data for law enforcement and security intelligence as a change in the field of security production. Chan (2003) has suggested that technological change can bring about changes in the field since technology is a much-valued resource. For example, in the field of policing, technology can be a 'power-amplifier' (Nogala 1995). Technical expertise can be a form of cultural capital: where previously police leaders were predominantly drawn from the criminal investigation branch, the ascendency of officers with IT expertise may threaten the traditional power structures of these organisations (Chan 2003). Technological change is, however, a double-edged sword. It can create problems and constraints for policing, such as leading to greater internal and external demands for information and putting limits on police discretion (Ericson and Haggerty 1997). Hence technological change can alter the field of security production by creating resources as well as constraints (positive and negative capital).

Technological change can also transform the habitus of security production. For example, the introduction of Big Data could bring about changes in security agents' assumptions about the purpose of information, what they regard as relevant information, how information is obtained

and used, and how they think information should be obtained and used (cf Sackmann's (1991) dimensions of cultural knowledge).

3. Research on Impact of Technological Change on Security Practice

There is a dearth of empirical research on the impact of technological change on security practice (Manning 2014:2512). What is available relates mostly to policing and law enforcement.

Chan's (2003) review of the literature found that while technological change in some instances can 'radically alter the structure of police organization by levelling hierarchies, blurring traditional division of labor, dispersing supervisory capacities and limiting individual discretion' (Ericson and Haggery 1997:388), it had generally resulted in continuities more than changes in police practices. For example, the availability of more data did not lead to a more proactive style of policing: police continued to regard 'information as useful only if it leads to arrests' and problem-oriented policing as 'soft' and 'marginal' (Chan 2003: 666). Similarly, what is relevant information was often restricted by police assumptions about the purpose of information, so that data on community profiles, economic conditions, community attitudes, etc was not usually regarded as relevant. Even though police were aware of the potential of using technology for 'smarter' policing strategies, 'they said there was not sufficient time or resources to realise this potential' (Chan 2003: 666). The availability of better information technology had also led to few changes in how information was obtained and used, and how police thought it ought to be obtained and used. For example, there was a 'cultural aversion' to depersonalised and decontextualised data generated by crime analysts (Cope 2003). Similarly, detectives had a tendency to 'co-opt crime analysis for the purposes of crime investigation' (Sheptycki 2004:324).

Chan (2003: 668) concludes that 'the prevalent attitude of police appears to still favour case-by-case investigation rather than crime analysis, evidence gathering rather than intelligence analysis, secrecy rather than openness in information sharing'. In fact, her study (Chan 2001) demonstrated a classic case of the clashing of technological frames between users (who expected technology to make their work easier) and architects (who had intended the organisation to use information in a more sophisticated way). Chan (2003), however, does not see technological frames as immutable. Rather, the introduction of new technology is 'merely the beginning of a "technological drama" (Manning 1992, 1996) of normalization, adjustment, reconstitution and reintegration' (Chan 2003: 673). Technological change can destabilise the status quo in terms of power balance, and can even lead to resistance or sabotage in some circumstances (Ericson and Haggerty 1997).

More recently published research similarly confirms that the impact of information technology on police practices can be uneven or unpredictable. For example, results of a multi-site study of police technology in the US demonstrate that 'the effects of technology are complex and that technological advancements do not always produce obvious or easy improvements in productivity, communication, cooperation, management, or job satisfaction' (Koper, Lum and Willis 2014:212). Similarly, research in six Canadian police services found that the use of 'crime science' and analytic technologies to support 'intelligence-led policing' (ILP) is more rhetorical than real (Sanders, Weston and Schott 2015:711). More specifically, the 'occupational culture of information hoarding… has shaped the use and functioning of police innovations' (2015:718). In line with previous research on the 'poorly understood and appreciated' role of crime analysts (eg Cope 2004), the lack of knowledge and training about crime analysis on the part of police managers and officers 'has rendered many analysts to engage in simple crime counting and mapping instead of advanced analytics' so that instead of adopting a new approach to policing (ILP), new technologies are used to support 'traditional modes of policing' (Sanders et al. 2015:724).

Nevertheless, with the production of security being a major global concern, public institutions such as police and national security agencies are the prime producers and communicators of security knowledge (cf Ericson and Haggerty 1997). There is therefore enormous pressure for these agencies to make use of new technological tools associated with Big Data.

4. Research Method

This article draws on a research project *Big Data Technology and National Security* conducted under the auspices of the Data to Decisions Cooperative Research Centre (D2D CRC). The empirical data includes 31 semi-structured interviews[2] conducted with 38 stakeholders including law enforcement and intelligence officials, policymakers, computer technologists, and officers in relevant civil society organisations. The research team worked with various government agencies and the D2DCRC's partners to identify potential interviewees in Australia. Twenty-four of the interviews were recorded with the consent of the research participants and verbatim transcripts prepared. For those who did not consent to recording, notes were taken to recreate as closely as possible the words used by research participants.

We classified research participants according to the nature of the organisation for which they worked. In each case, there were three potential classifications: Operational (O), Technical (T) and Policy (P). Where a participant was being interviewed in relation to a recent former role, the coding matched the former organisation. While participants were asked different questions depending on their role and organisation, all participants were asked similar questions in relation to their framing of Big Data.

Among the 38 participants, 19 were from operational, 7 from technical and 12 from policy organisations. Since the sample was not randomly selected, the results presented here should be regarded as indicative rather than representative of the population of stakeholders. Another limitation of the sample is that interviewees from operational organisations were mainly in managerial or higher positions rather than security agents operating at the coalface. This was in spite of our request to have both managerial and operational officers represented.

Quotations from interviews have been altered in various ways. In order to protect the identity of research participants, any details of their organisation or team that appeared in the transcript were removed. In order to increase the fluency and relevance of selected quotations in the report, we have also used ellipses and square brackets to indicate the omission or replacement of words respectively.

In accordance with the framework described in Part 2, the following analysis will focus on several dimensions of security agents' habitus: their perception of the purpose of data in general, their conception of Big Data and its capability and value, and their expectations of how Big Data will affect their work. It will also discuss participants' perceptions as to how the field of security production is likely to be affected, i.e. the winners and losers in the use of Big Data.

5. The Purpose of Data

Data may be regarded as a form of 'security object' that is relatively banal (i.e. commonplace and taken for granted) yet powerful nevertheless (Goold, Loader and Thumala 2013). Research participants in our study worked with a wide range of data, from telecommunication metadata, official data, data from international partners, internal databases, information provided by the community, geospatial or financial data to open source or online data and communication signals.. Not unexpectedly, the purpose of data was very much tied to investigations:

> Any data that we can collate online, whether it be that online evidence *that may indicate the commission of offence or assist in making a nexus, a link, to that offence*, such as photographs, emails, whether it be data these days, obviously text messages, contacts. Realistically it's comprised of anything that's online that we can, again lawfully, collate *for the purpose of our investigation*… we use any data that we can get our hands on lawfully, certainly, *to assist in our investigation*. (O, emphasis added)

In terms of the *temporal scale* (Valverde 2014) of their security projects, research participants from operational organisations nominated a range of past-focused and future-oriented purposes of using data. Past-focused purposes include investigation, arrest and prosecution (nominated by 9 participants), reporting (1), and event evaluation (1); while future-oriented purposes include prevention or disruption of incidence or mitigation of risks (6), intelligence gathering (4), identification of trends or risks (3), policy or service decisions (3) and trust building (1). Often, data would serve multiple purposes, such as:

> [Data is mainly used for] security intelligence. You're looking at two or probably three areas. One is *event prevention*, so trying to foresee something or stop something from happening. Two, you're looking at *event evaluation*, so what happened and now retrospectively that we know something has happened—can we better analyse it to see what we missed, what we could have done better around who was involved now that more players might be exposed? Then I guess the third one was creating the bigger picture, so you find one person of interest and then you look at 10 people that they regularly contact and you look at the 10 people that they regularly contact and then you look at the 10 people they regularly contact and you create a global map or an organisational map of contacts and then you … cut out who's not of interest…. Then you start to look for the links across the networks … so that informs then this *strategic analysis* … it's that kind of longer term analysis rather than event based analysis. (O, emphasis added)
>
> Yeah, we talk about a spectrum of activity. So we've got … traditional law enforcement so we always go for *prosecution*. If we can't prosecute … depending on where it is in the cycle, we'll look for an *intervention* like a control order or a preventative detention order … Then we'll go into the middle where we're looking at this sort of *disruption* thing. … So you have to sit back, bring that data together and actually work out what's the risk we're going to have and how are we going to play that? What's the way to intervene? (O, emphasis added)
>
> We do what we call *security intelligence investigations*. In the course of that, we produce lots of intelligence … It depends on the national security outcome we are trying to achieve. We deal very much in shades of grey. Jail may be the best national security outcome where police assisted by [name of agency] have enough evidence to *put someone in jail*. But in some situations, it may be just as good to stop them doing something. We can sometimes convince them to stop, that is, *disruption* that does not involve prosecution. (O, emphasis added)

As one research participant noted, the purpose of using data was not static but potentially evolving:

> [W]e're very focused on prosecution. There's a real desire within parts of the agency to move away — certainly with some crime types — move away from prosecution and be more imaginative in terms of the strategies around disruption, deterrence, target hardening and the likes. … But if we weren't so focused in on prosecution all the time, I suggest that we would look for different data sources and we would ask different questions of the data, because we'd have a different mission if you like. (O)

This highlights that different missions involve different data and different tools. For example, investigation and disruption both involve identifying individuals to whom data pertains. Even where research participants described using data for future-focused activities, the kind of analysis being done very much revolved around investigating individuals for past conduct or identifying individuals who may be involved in future conduct rather than understanding broader trends among groups. This is consistent with the fact that almost all research participants were only interested in *identified*, rather than *de-identified* data:

> Rarely is it de-identified, because the only reason we'd be sharing information is for investigative action or in support of an investigative outcome. … [T]he purpose … is to identify who, what, where, how, etc. … [I]t has to be for the purposes of the conduct of an investigation with an intent to prosecute, and where all other avenues have dried up. (O)
>
> It's no value if it's de-identified. (O)

With few exceptions, where sharing of de-identified was discussed, it was generally as a future possibility or rare practice:

> It is possible that, in the future, police could use our data to predict trends....(O)
>
> We typically share reports … reports based on identified, classified data. (O)

This was consistent with accounts of participants from technical organisations who stated that their systems are not concerned with de-identifying data or that such data is not of central interest to government clients:

> The systems that we're currently looking at aren't trying to de-identify data. (T)

> We don't provide the capability to de-identify data. (T)

The above findings suggest that the importance of using data for case-by-case, investigative or disruptive purposes, rather than for identification of trends, predictions, or strategic analysis, is a shared assumption among security agents, a key dimension of their habitus, even at the managerial level.

6. Big Data and Its Capability and Value

To understand how agents in the field of security production conceived of Big Data, we examine what they thought Big Data is and what capability and value it will bring to their work.

Definition of Big Data

Research participants were asked how they would define Big Data. This was done not to measure awareness of a fixed definition, but rather to explore diverse interpretations of a flexible concept. Figure 1 shows the main responses broken down by the type of organisation participants worked in. The most frequently mentioned attribute of Big Data was in terms of its volume, followed by its analytic or predictive capacity, the fact that it consists of aggregated or integrated data from different sources, and that the volume of data makes its handling beyond the capacity of humans, the skills of existing analysts or current technology. Some mentioned velocity and variety as characteristics of Big Data. Five participants—all from technical organisations—saw Big Data as a marketing term that covers a variety of techniques. Only two participants mentioned veracity as a challenge of Big Data.

[Figure 1 about here]

Volume was often mentioned together with the need for new technology, particularly in relation to the need to employ advanced techniques in analysis:

> An ever-increasing, an exponentially-increasing volume of information which is beyond the capability of a human to analyse without computer assistance. (O)

> My understanding is Big Data is enormous data sets or combinations of data sets that require advanced and analytic techniques in order to make sense of them or analyse them. (P)

Some participants saw the analytic capacity of Big Data, the capacity to 'unlock the secret that's within the data' (O), as its defining feature:

> I would describe Big Data as the consolidation of large amounts of information in a single or multiple repositories that can be manipulated or explored to release information or findings that could not be found if the data [were] analysed individually or separately. It's primarily associated with trying to find much more complicated, complex relationships – it's this trying to unlock the secret that's within the data. (O)

While four of the participants from technical organisations mentioned volume as one of the characteristics of Big Data, five of them admitted that they disliked the term Big Data which some saw as a marketing term. They would prefer to focus on analytics or predictive techniques—the size of the dataset may or may not be essential:

> Big data is something that's obviously more of a marketing term than anything specific … Big data means I guess the collection and exploitation of significant volumes of data to drive outcomes that are relevant to the business or organisation that is trying to use it ... I think Big Data can be a bit of a distraction because it's not so much necessarily about the volume of data but about the signal in the data that's actually of primary interest … ultimately it's the analysis and that cuts across both what you might term analytics… to derive whatever the outcomes are that are relevant for the situation that you're working through. (T)

Almost one in four research participants defined Big Data in terms of the aggregation or integration of data from different sources. The majority of these worked in operational organisations:

> So Big Data is everything — because I actually consider what we hold, agencies, as Little Data. The Big Data that's out there is a lot of the stuff that sits in the public space, like Facebook, like Twitter and things like that. Then you move to the next phase which data being held on all of us which is held in different sort of areas like our licensing material, our passports material, our movements material. All this sort of stuff that sits in silos which when analysed on its own really means nothing but when you aggregate it all up can actually build a pretty good picture about somebody. (O)

> …it's the accumulation of large datasets beyond what would normally be held within one organisation or entity containing many different aspects of information within that dataset. Therefore the analytics of it is how can you identify those useful pieces of connections between those disparate pieces of information. (O)

Thus Big Data can generate diverse meanings among those working on or formulating policies for security projects. As well as the obvious question of size, the term captures ideas about analytic capacity, the integration of data sets, the technological horizon and buzz word scepticism.

Capability and Value of Big Data

Research participants were also asked questions designed to elicit their perceptions as to the capacity and value of Big Data, particularly for law enforcement and security intelligence (see Figure 2 for the distribution of responses).

[Figure 2 about here]

Half of the participants referred to Big Data's more advanced analytic capacity:

> Most importantly I think predictive trending potentially. Retrospective networking or even real-time networking analysis. Associational analysis of individuals, groups, and organisations. (O)

> What makes it different is that increasingly using better tools and techniques we can gain insight from data that to date are not humanly possible. So it helps us join the dots where we can't possibly do it ourselves. (O)

A smaller proportion mentioned its 'richness' or 'completeness' as the advantage of Big Data, which was then linked to its analytic capacity:

> So what these big data analytics allow you to do is to use all of your data, rather than a subset… and therefore get a much more complete picture of what's there, and therefore get much more valuable and highly qualified insights. The other is that it allows you to implement a lot more real time analytics… So that's the big change really. (T)

> The difference is between populational data as opposed to a sampled data set. If you have complete data, the potential for analysis is not subject to the risk of modelling but is observed fact. In other words, richer analytical capacity. (P)

The 'richness' of Big Data was also linked to an investigative advantage by participants who worked in operational organisations, by providing historical and contextual details, as well as the ability to cross-check information and identify new targets:

> … let's say for example we were analysing past activities of what terrorist suspects have been like. So analyse their movements against when they applied for their passports, who went guarantor for them, where they went to school, what their license is, when they got it, all that sort of stuff and we analysed all that for individuals. Out of that we might be able to pick up some patterns. … Then if you … develop an algorithm from that and then you ran it right across all the systems you may very well pick up targets that are previously unknown to us … So using … an analysis of previous data in terms of predictive type activity. None of us have the capability to do that at the moment even though the information is probably out there to do so. (O)

> [Big Data's] interrogation potential. You can cross check against multiple things. (O)
>
> You can actually build profiles and identify people, patterns of life, things like that. I mean … that actually gives you a greater level of understanding about somebody before you actually approach them. … Whether we're setting up a surveillance plan or we're planning when we're going to execute a search warrant and all those sorts of things which are traditional law enforcement, trade craft which we do for a whole range of reasons, a lot of it around safety and our own people in the broader community, but also about actually understanding … a situation. Because while it gives you the opportunity to target in on people it also gives you the opportunity to not target people … (O)

Four out of the seven research participants who worked in technical organisations and two from the policy group mentioned proactive/preventative policing as an opportunity that Big Data could open up for law enforcement and security intelligence:

> In the counter-terrorism space it's going to be manifested through a better ability to prevent – although you can never prevent but to be able to intercept, detect and otherwise intervene in potential events before they happen. (T)
>
> The biggest one, I think, is prediction and probably the most challenging. Trying to change the way policing works so that it's not reactive, but is more proactive about looking for potential anomalies or indicators that something might be occurring. (T)
>
> I guess the shift that everybody talks about, which I think is a reasonable way of putting it, is to move towards preventative policing and preventative law enforcement national security. In other words not to react to an occurrence, but to be able to anticipate occurrences, anticipate where law enforcements resources may be required ahead of time. So to move from a lagging indicator regime to a leading indicator regime. (T)

Surprisingly, this was not mentioned by any of the research participants who worked in operational organisations, not even those in a technical role. This suggests that there may be an incongruence between the technological frames of the operational and those of the technical participants. Participants in operational organisations saw the investigative advantage that Big Data could bring, but participants from technical organisations were suggesting that Big Data could offer a different way of doing policing and intelligence work.

Improved efficiency or effectiveness was mentioned by six research participants as what Big Data can provide. Four participants (three were from technical organisations) pointed to the opportunity for governments to make better decisions or provide better services, while three mentioned confidence or accuracy as an advantage of Big Data. One participant with an operational role cautioned against having unrealistic expectations about the predictive capability of Big Data in the context of crime. Finally, one participant (from the policy group) confessed they didn't know what the advantage of Big Data was.

More than half of the security agents who took part in the research said that they were not currently using Big Data. This suggests that their conceptions of Big Data and its capability and value were not necessarily based on first-hand knowledge or experience with this technology. In spite of the small sample sizes, the apparent *incongruence in technological frames* between the operational and the other (technical and policy) participants is consistent with the findings in Part 5 that an important dimension of the habitus of security agents was their shared assumption that data was useful for case-by-case investigative or disruptive purposes in relation to known events or individuals, rather than for predictive modelling to anticipate new threats. This raises another question about their habitus: what do security agents expect from Big Data technology? This is examined in the next Part.

7. Expectations regarding Big Data

Our interviews with operational participants suggest that security agents have different expectations about what Big Data technology will bring. Since more than half of them had not been using Big Data in their work, the advent of Big Data has created a 'occasion' for a new focus for sensemaking, which, as Weick (1995: 14) argues, is to 'construct, filter, frame, create facticity … and render the subjective

into something more tangible'. To use Bourdieu's terminology, sensemaking is the process through which the habitus constructs and interprets changes in the field.

Participants were both attracted to new technology and wary of what it may bring. To make sense of this new scenario, 'they simultaneously interpret their knowledge with trusted frameworks, yet mistrust those very same frameworks by testing new frameworks and new interpretations' (Weick *et al.* 2005: 412). Trusted frameworks can be based on traditions or standard procedures, naïve expectations or informed understanding, familiar experience or a leap of faith. As one technologist participant pointed out, unrealistic expectations can lead to 'pretty bad outcomes':

> I think there are risks around expectations … historically in [technical organisation] we've talked about it as the 'find terrorist' button. …[O]ur organisation was working on counter-terrorism problems and probably for the first three or four years of our existence the most requested feature was some manifestation of which button do I press to actually find the bad guy? There is, particularly among non-technical people, a yearning desire based on movies and otherwise to actually think that there is an ability to just automatically do their job for them. The reality is that that's far, far from the truth and far, far from desirable … So there's a risk that the expectation will never be met and there's a risk that the expectation is just misguided to begin with. … There's no substitute for having an intelligent human being in their intuitions and understanding of the world and you very much… want that person to be there. There's a risk that that is not well understood and there's a risk of software companies coming to the table and saying, well, technology is the answer and due to that mismatch of expectation too much willingness on behalf of these agencies to accept that as true which could ultimately have pretty bad outcomes. (T)

Some participants focused less on capability and more on the ability to use the tools conveniently, referencing features like mobility and speed:

> More and more they want the data immediately or in real time. … [A]t least some agencies are moving towards the need to have data on device when out on the streets when doing their job. (O)
>
> That comes down to again speed access to that data, to download that or to upload that information, and to access it, and capacity. (O)

This perspective is very much grounded in existing frameworks and modes of practice.

Given the importance of case-by-case investigation or disruption of crime or disorder, operational participants who considered capability improvements generally expected Big Data to bring more diverse data (as implicit in the understanding of Big Data as data aggregation), and thus were concerned that it also comes with better facilities for sorting or prioritising information, which may require a higher degree of automation:

> Law enforcement organisations are thirsting for more data and the right data at the right time. They are nervous about being swamped with data so getting right data is important. (O)
>
> What you want is that if there are a thousand pieces of information we want the analytical tools to do the analysis, to understand the context and prioritise to say do this one first, this one second, this one third ... (O)
>
> [T]he amount of Big Data that that is going to create is very large but there's going to be a lot of useful information in there and an extreme amount of un-useful information. So our ability to gain access to that data and have a mechanism to find the needle in the haystack or the valuable information from the rubbish is going to be extremely important. (O)

Related to the idea of better sorting was improved tools for human-driven search and data exploration. These were generally framed by comparisons with existing and familiar commercial products, such as Google and IBM Watson, sometimes by direct reference and sometimes by similarly described functionality:

> There is no capability to put in a name and draw from various different sets of data – No POOGLE [Police Google]– can't put in a name and get an answer like you can with Google. (O)

> Big Data will come alive when it adapts to what is being searched for, once you get into the first layer, you get further result sets getting the spider's web of structured index data, it self-learns machine-learns each time but we don't really have this yet. (O)

> The thing that struck me about Watson … is you get to a point where [you have set up the appropriate rules] then you should be very comfortable that the more data you provide to an engine like that, … it would take you to the answer of that question, … it gives you better surety about the judgements you make about what's going on in the environment. Or what might be going on in the environment, or what might go on in the environment sometime in the future. Or what might have gone on in the environment that you don't have real visibility of. (O)

Again, as with the case of sorting and prioritisation tools, there was an expectation of increased automation. However, a number of participants thought that fully automated Big Data tools would not be effective and emphasised the importance of human evaluation and reasoning as part of the process, so that automation would assist rather than replace human analytic reasoning:

> You need a system flexible enough to show near hits and create associations but a person makes the decision. (O)

> I would be cautious about relying on anything computer generated to gain a complete understanding about intent and so forth. Not in my lifetime. (O)

> I think one of the greatest things [Big Data] can deliver to law enforcement and to the national security community agencies is reducing the amount of time that humans spend curating data, managing data, getting it into the right formats and into the right places before they analyse it. The most critical thing that new tools, techniques and procedures in big data analytics will do for those agencies is to increase the amount of time analysts spend analysing rather than managing data. (O)

> I think there is a risk that smart systems will deskill people. It scares the hell out of me. (O)

There is thus some realisation among operational participants that, as much as automation of some functions is useful and necessary in the context of large, diverse data sets, a 'find terrorist' button is both unlikely and undesirable.

While most participants linked their projections to trusted frameworks and existing practices, one participant from an intelligence organisation described how a 'Big Data' business model would change their current operation:

> We operate under a 'join the dots' business model. … If we have a lead, we follow the lead to its logical conclusion, joining the dots. We don't access data until we have cause to use it (need to link another dot). … Under a Big Data business model, we [would] have all the data available all the time, we traverse it constantly looking for trends, patterns, anomalies and red flags. (O)

According to this participant, Big Data would change the approach to how intelligence work is done. Interestingly, however, the use of 'we' as a subject of the verb 'traverse' suggests that this process would be human, not machine, driven.

What is important to note here is that, outside the contexts of technologies for prioritising and decrypting data, and possibly distributed data storage systems, none of the future visions described by the security agents would involve significant technological breakthroughs. Much of it draws on existing commercial tools, such as Google search or IBM Watson. This is unsurprising – agents made sense of the possibilities of Big Data technologies in light of what they understood about existing technologies. Mostly, agents were concerned with new ways of doing things that can be linked to better access to more data, being permitted to use it in new ways, better IT resourcing (for example, through mobile access and faster speeds), or better project management. They wanted more data, but also the tools to manage it. Mostly, they wanted to use data to make their work easier (e.g. tools

that can be accessed quickly and remotely, better prioritisation of information, better search functionality) rather than to change the nature of their work (e.g. from investigation, prosecution or disruption of individuals to broader identification of trends). A notable exception is the suggestion that intelligence could move from 'joining the dots' to Big Data approaches. There were some general concerns about negative implications of Big Data thinking, and some more specifically linked to excessive automation (which raises issues of job losses and thus reduced status for current employees as well as questions about the quality of decision-making). But overall, agents were looking to existing, commercially available technologies in imagining the future of Big Data technology in their own work.

8. Winners and Losers in Technological Change

The field of security production is made up of a multitude of agencies and agents charged with responsibilities to maintain order and security, preventing crime and protecting people and property. Big Data technologies are likely to be taken up to different extents by different agencies depending on their capacities, resources and purpose. The fact that not all intelligence and law enforcement agencies had equal capacity to access Big Data technologies was noted by two research participants:

> … there is a broad spectrum of sophistication across the law enforcement and … the national security community or agencies … So within the national security community there's a vast difference in the maturity and sophistication of the use of Big Data and Big Data analytics. (O)

> …it's very largely a question of resources. The intelligence services have many more resources proportionately speaking than the police do for this kind of work. (P)

Resources and capabilities can be a source of prestige, both for the agencies themselves and security agents within them.

As discussed in section 2, technological change can be a resource as well as a constraint, providing advantages to certain groups while posing risks for others. We asked all participants to identify the risks of using Big Data for law enforcement or security intelligence. The risks identified are set out in Figure 3 and they vary by the type of organisation participants represented. While those from operational organisations mentioned most of the listed risks, only two mentioned misuse of data. Participants from policy organisations were most concerned with privacy, data security, and misuse of data, with no more than one person mentioning any of the other identified risks. Those from technical organisations were most concerned with misuse of data and misplaced trust in Big Data technology. Overall, privacy, data security and integrity, misuse of data and misplaced trust in technology or algorithms were the most significant concerns, while only one research participant was concerned about the risk of discrimination.

Differences among the three groups are interesting, while not surprising. Those in operational organisations seemed to be less concerned about misuse of data and more concerned about their own potential loss of capital (through political and reputational risks, lower public perceptions and overload) compared to other groups. More surprising is the fact that those in operational and technical organisations were conscious of misplaced trust in technology, an issue of less note to those in policy organisations (which include government agencies focussed on policy). Also surprising is the relatively low level of concerns around the potential for discrimination, despite these being raised in the literature (Barocas and Selbst 2016).

[Figure 3about here]

For research participants in operational organisations, *not* engaging with Big Data technologies could itself be a risk:

> The real question is what are the risks of not taking a Big Data approach. … Whether [the public] are comfortable on a bulk data perspective, if we don't have access to data we cannot stop things happening. It is about national security outcomes. We know people want to breach national security. If the data is there, we will be able to stop terrorism or espionage (O)

Yet having access to Big Data also presents a risk to operational participants: agencies could face a loss of symbolic capital (e.g. public trust, reputation) if they did not act on the data they had, they made use of data that 'society didn't think they had access to', or they acted on a 'false positive':

> Again, that's probably one of the *biggest risks*, I think, of Big Data, that from an organisational point of view, if you know something you haven't acted on that information, therefore are you liable in the public sphere that you knew the risk and you did nothing with it, regardless of where that data sits, or where that risk sits. (O, emphasis added)
>
> I think there's a risk for the police and law enforcement and intelligence agencies — really about perception. If they are seen to be using data that society didn't think they had access to. (T)
>
> I think a reasonable paranoia on the part of the law enforcement national security agencies themselves is the embarrassment of a false positive. A lot of the sophistication in the system really is about reducing the number of false positives, and for that matter of false negatives. So that's an area that gets a lot of attention. That's really an area where you might even end up catching totally innocent people, just through a set of circumstances that made a suggestion that turns out to be unwarranted. (P)

While risks to agencies dominated among operational participants, all categories of research participants identified more general risks . The most frequently mentioned concern was that 'everyone, the community or citizens' were exposed to the risks of using Big Data. The risks here were largely around privacy, poor data integrity and security and misuse of data, including the risks of 'vendetta policing', harassment and over-enforcement. Other categories of people exposed to risks include minorities and people at the margins, people of interest to law enforcement and security agencies, academics and researchers, and people identified through data.

The analysis above suggests that technological change in the 'game' of security production generates both winners and losers. Stakeholders, including security agents, were cognisant of the range of risks Big Data technology could bring to the field of security production, e.g., the risks of invasion of citizens' privacy, compromises to data security and integrity, misuse of data, misplaced trust in technology, and various political and reputational risks to governments and security agencies. Yet for security agents, these risks must be weighed against the potential benefits of Big Data, at least as they understood them.

9. Conclusion

In spite of the promises of Big Data for improving the efficiency and effectiveness of policing and security agents, very little is known about how Big Data is understood or imagined by these agents. Empirical findings from our Australian study suggest that Big Data is a security technique that is both novel and contested (cf Goold et al. 2013). Less than half of the security agents who participated in the research reported that Big Data was being used in their unit; their conception of Big Data was therefore not necessarily based on experience with this technology. Different stakeholders perceived the value of Big Data in slightly different ways: while all participants emphasised its analytic capacity, security agents tended to focus on the richness of data and the investigative advantage it affords, while participants in policy and technical organisations saw Big Data as opening up opportunities for a more proactive approach to security based on inferences from trends and patterns. This is consistent with an important dimension of the habitus of security agents: while data was considered useful for both past-focused activities (e.g. detection and investigation) and future-oriented exercises (e.g. prevention, disruption or risk reduction), the focus was almost always on identifying and learning about individuals rather than understanding broader trends. Security agents expected Big Data to provide better access to more data and a range of improvements over current methods, without any fundamental change in approach. Their visions of what Big Data could offer were primarily based on their current technological frames and their experience with existing commercial tools. While they were aware of community concerns around issues such as privacy and data security, they were especially conscious of the political and reputational risks in raising public expectations and not delivering the outcomes through technical or human errors.

Valverde (2014: 389) has argued that it is 'dangerous' to focus on techniques only in our analysis of security projects, as their logic, scale and jurisdiction 'cannot be read off from the techniques'. Our analysis confirms this — stakeholders have different expectations of what Big Data can provide as a security technique. While security agents may see the purpose of using data as split between (past-focused) detection and investigation and (case-based future-oriented) prevention or risk reduction, among developers of software tools, the 'selling point' of Big Data analytics has primarily been future oriented and risk-based rather than case-based (see Bennett Moses and Chan 2016). This potential incongruence in technological frames between the users and the architects of Big Data is likely to pose problems for future implementation. Thus, technologists could pay more attention to their own expectations and assumptions and whether they are aligned with those of users and managers (Orlikowski and Gash 1994).

A better understanding of how cultural assumptions (part of habitus) can influence the impact of new technology is not only important for managing technological change within organisations, but also for designing regulatory or governance regimes (other techniques of security) for the benefit of the broader community. Goold et al.'s (2013:987) analysis of how surveillance cameras in the UK have become a banal security object, taken for granted by citizens as 'an integral part of the infrastructure of public life', even a new kind of 'security blanket', should alert us to the possibility of the 'securitisation' of Big Data going down the same path, either through ignorance or apathy.

There are many potential futures for greater use of Big Data in national security, both from the perspective of potential access to larger, integrated datasets, and the increased capacity to extract information from data. There are also a number of risks associated with different pathways, which will affect the likelihood and extent of impact on the potential 'losers' here. The habitus of different players in the field is crucial because it will affect how security practices change in response to Big Data ideas. Because of the diversity among stakeholders, the outcome is partly a question of jurisdiction in Valverde's sense, and not only of the technical performance of the various possibilities. Our study has revealed where there are gaps in participants' understandings of risks or impact on capital. For example, while there is an awareness within operational organisations of the limits of fully automated decision-making, there is also a strong sense that algorithms can be used to prioritise targets and perhaps even identify new ones. Surprisingly, only one research participant (from the policy group) raised the issue of discrimination as a risk in this context. The study thus also suggests that, while arguments about privacy are familiar (although subject to disagreement), other risks are either unexplored or only considered within particular types of organisation. If Big Data is to make a difference to security practice, there needs to be greater alignment among sectors regarding understandings of the technologies involved, whether and how they ought to change approaches to security, and, most crucially, where the risks lie and how negative impacts can be diminished.

Funding

This work was supported the Data to Decisions Cooperative Research Centre (D2D CRC) [DC52001].

Acknowledgment

The authors would like to thank Professor Louis de Koker and Dr Alana Maurshat for contributing to the project design and the fieldwork. We also thank the D2D CRC for their assistance with the recruitment of research participants. The valuable research assistance provided by Daniel Cater and Brigid McManus is also gratefully received. We thank all research participants for their generosity in responding to our invitations and Gavin Smith for his insightful comments on an earlier draft of this article. The views expressed in this paper do not represent those of the D2D CRC.

References

Barocas, S. and Selbst,A.D. (2016), 'Big Data's Disparate Impact', *California Law Review*, 104, forthcoming.

Bennett Moses, L., and Chan, J. (2014), 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools', *University of New South Wales Law Journal*, 37: 643–78.

Bennett Moses, L., and Chan, J. (2016), 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability', unpublished paper.

Bijker, W. E. (2010), 'How is Technology Made? – That is the Question!', *Cambridge Journal of Economics*, 34: 63–76.

Bourdieu, P. (1987), 'What Makes a Social Class? On the Theoretical and Practical Existence of Groups', *Berkeley Journal of Sociology*, 32: 1–18.

boyd, d., and Crawford, K. (2012), 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon', *Information, Communication and Society*, 15: 662–79.

Chan, J. (2001), 'The Technological Game: How Information Technology is Transforming Police Practice', *Criminology and Criminal Justice*, 1: 139–59.

Chan, J. B. L. (2003), 'Police and New Technologies', in T. Newburn, ed., *Handbook of Policing*, 655–79. Willan.

Chan, J., and Bennett Moses, L. (2016), 'Is Big Data Challenging Criminology?', *Theoretical Criminology,* 20: 21–39.

Cope, N. (2003), 'Crime Analysis: Principles and Practice', in T. Newburn, ed., *Handbook of Policing*, 340–62. Willan.

Davidson, E. (2006), 'A Technological Frames Perspective on Information Technology and Organizational Change', *Journal of Applied Behavioural Science*, 42: 23–39.

Ericson, R. V., and Haggerty, K. D. (1997), *Policing the Risk Society*. Oxford University Press.

Goold, B., Loader, I and Thumala, A. (2013), 'The Banality of Security: The Curious Case of Surveillance Cameras', *British Journal of Criminology*, 53: 977–996.

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

Koper, C.S., Lum, C. and Willis, J.J. (2014), 'Optimizing the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behaviourial Aspects of Implementing Police Technologies', *Policing*, 8(2): 212–221.

Mackenzie, D., and Wajcman, J. (1985), *The Social Shaping of Technology: How the Refrigerator got its Hum*. Open University Press.

Manning, P.K. (2014), 'Information Technology and Police Work', in G. Bruinsma and D. Weisburd, eds., *Encyclopedia of Criminology and Criminal Justice,*2501–2513. Springer.

Manning, P. K. (1992), 'Information Technologies and the Police', in M. Tonry, and N. Morris, eds., *Modern Policing – Crime and Justice: A Review of Research*, vol. 15, 349–98. University of Chicago Press.

Manning, P. K. (1996), 'Information Technology in the Police Context: The "Sailor" Phone', *Information Systems Research*, 7: 52–62.

McCahill, M. (2015), 'Theorizing Surveillance in the UK Crime Control Field', *Media and Communication,* 3(2):10–20.

Nogala, D. (1995), 'The Future Role of Technology in Policing', in J. P. Brodeur, ed., *Comparisons in Policing: An International Perspective,* 191–210. Aldershot: Avebury.

Olesker, A. (2012), 'White Paper: Big Data Solutions for Law Enforcement'. CTOlabs.com, available online at http://ctolabs.com/wp-content/uploads/2012/06/120627HadoopForLawEnforcement.pdf.

Orlikowski, W. J., and Gash, D. C. (1994), 'Technological Frames: Making Sense of Information Technology in Organisations', *ACM Transaction on Information Systems*, 12: 174–207.

Podesta, J., Priztker, P., Moniz, E. J., Holdren, J., and Zients, J. (2014), *Big Data: Seizing Opportunities, Preserving Values*. Executive Office of the President (US), available online at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Sackmann, S. (1991), *Cultural Knowledge in Organizations*. Sage Publications.

Sanders, C.B., Weston, C. and Schott, N. (2015), 'Police Innovations, "Secret Squirrels" and Accountability: Empirically studying intelligence-led policing in Canada', *British Journal of Criminology*, 55: 711–729.

Sheptycki, J. (2004), 'Organizational Pathologies in Police Intelligence Systems: Some contributions to the lexicon of intelligence-led policing', *European Journal of Criminology* 1(3): 307–332.

Staniforth, A., and Akhgar, B. (2015), 'Harnessing the Power of Big Data to Counter International Terrorism', in B. Akhgar, G. B. Saathoff, H. Arabnia, R. Hill, A. Staniforth, P. Bayerl, eds., *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, 23–38. Elsevier.

Swartz, D. (1997), *Culture & Power: The Sociology of Pierre Bourdieu*, Chicago: University of Chicago Press.

Valverde, M. (2014), 'Studying the Governance of Crime and Security: Space, Time and Jurisdiction', *Criminology & Criminal Justice*, 14: 379–91.

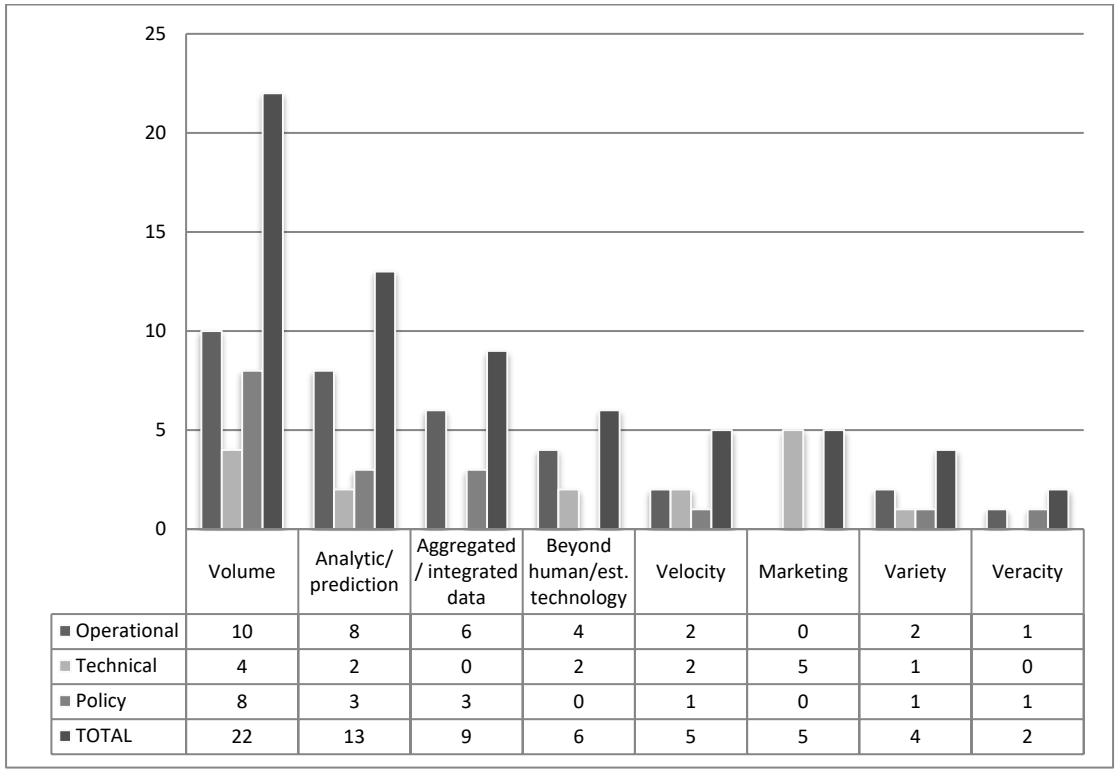
Weick, K. E. (1995), *Sensemaking in Organizations*. Sage Publications.

Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. (2005), 'Organizing and the Process of Sensemaking', *Organization Science*, 16: 409–21.

Wyllie, D. (2013), 'How "Big Data" is Helping Law Enforcement'. PoliceOne.com, available online at https://www.policeone.com/police-products/software/Data-Information-Sharing-Software/articles/6396543-How-Big-Data-is-helping-law-enforcement/.

Tables and Figures

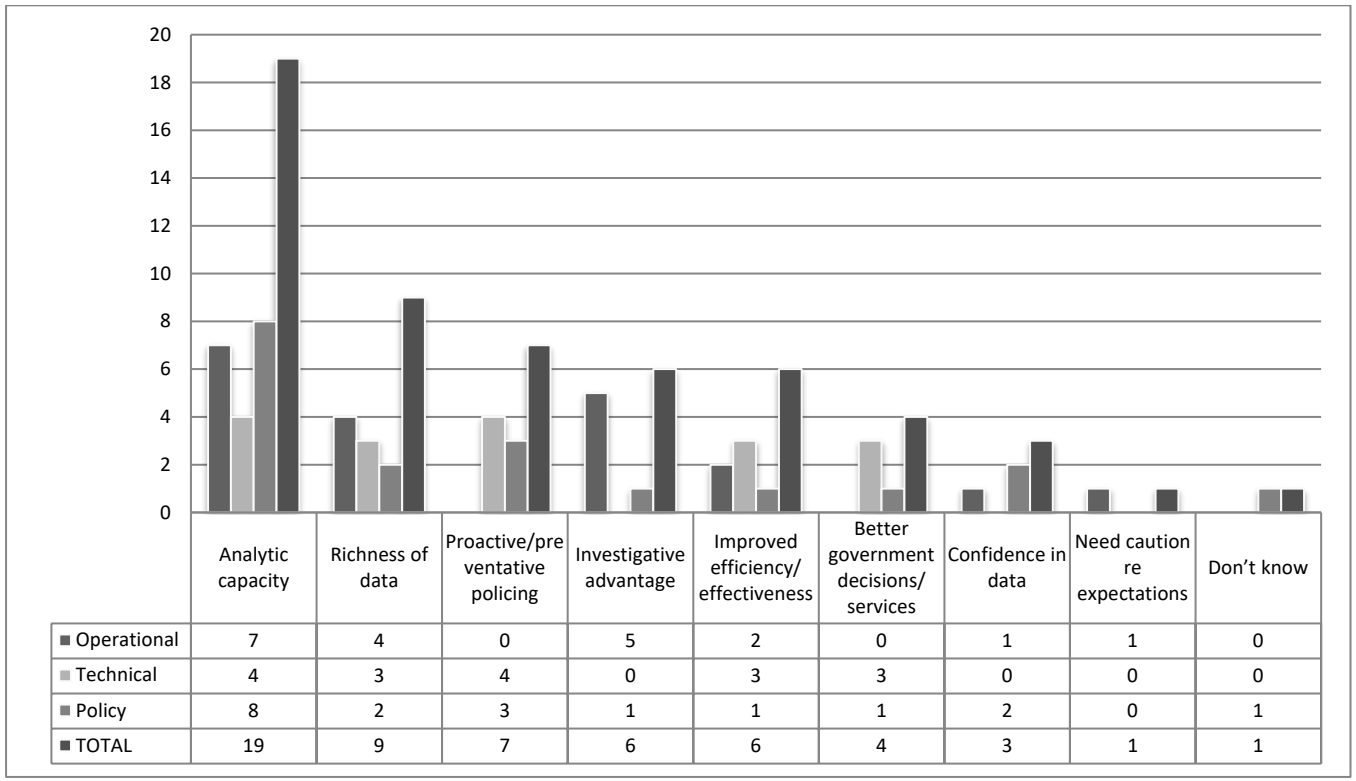
Figure 1 Conception of Big Data by Type of Organisation Employing Participants (n=38)



	Volume	Analytic/ prediction	Aggregated / integrated data	Beyond human/est. technology	Velocity	Marketing	Variety	Veracity
Operational	10	8	6	4	2	0	2	1
Technical	4	2	0	2	2	5	1	0
Policy	8	3	3	0	1	0	1	1
TOTAL	22	13	9	6	5	5	4	2

*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

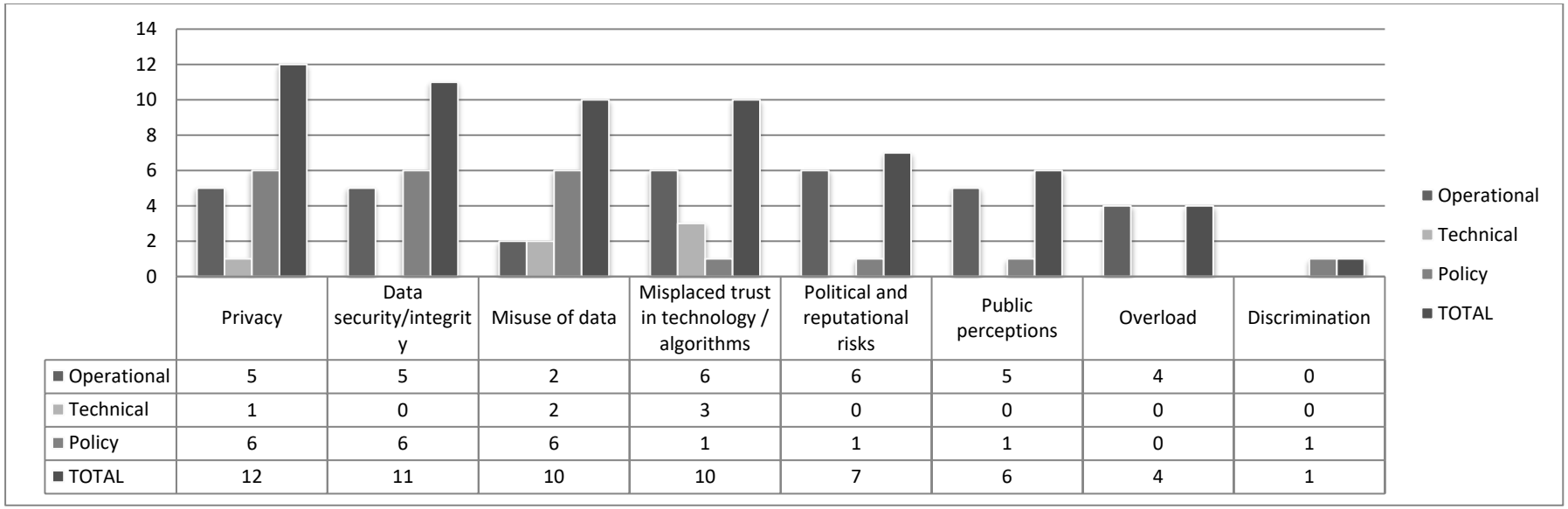
Figure 2 Perceived Capability and Value of Big Data by Type of Organisation (n=38)



	Analytic capacity	Richness of data	Proactive/preventative policing	Investigative advantage	Improved efficiency/ effectiveness	Better government decisions/ services	Confidence in data	Need caution re expectations	Don't know
Operational	7	4	0	5	2	0	1	1	0
Technical	4	3	4	0	3	3	0	0	0
Policy	8	2	3	1	1	1	2	0	1
TOTAL	19	9	7	6	6	4	3	1	1

*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

Figure 3: Risks of Using Big Data by Research Participant Organisation (n=38)



	Privacy	Data security/integrity	Misuse of data	Misplaced trust in technology / algorithms	Political and reputational risks	Public perceptions	Overload	Discrimination
Operational	5	5	2	6	6	5	4	0
Technical	1	0	2	3	0	0	0	0
Policy	6	6	6	1	1	1	0	1
TOTAL	12	11	10	10	7	6	4	1

*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

Notes

[1] Orlikowski and Gash's (1994) notion of 'technological frames' differs from Bijker's (1995) in that the former involves socio-cognitive structures, whereas the latter involves only social structures (see Davidson 2006: 37).

[2] The project received human research ethics approval from the universities involved in December 2014.