doi:10.1093/bjc/azw059 BRIT. J. CRIMINOL. (2017) **57**, 299–319
Advance Access publication 9 August 2016

MAKING SENSE OF BIG DATA FOR SECURITY

JANET CHAN* and LYRIA BENNETT MOSES

Big Data technologies hold great promise for improved efficiency and effectiveness for law enforcement and national security. This article explores the potential impact of Big Data on the production of security in society. 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 reveals the expectations and anxieties regarding Big Data among stakeholders and concludes that the community should take a more active role in understanding Big Data and influencing the governance of its usage.

Keywords: Big Data, Bourdieu, law enforcement, security intelligence, sensemaking, technological frames

Introduction

'Big Data' is an amorphous concept that has been used to refer both to large, diverse, rapidly changing datasets and 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 to use '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. Ultimately, Big Data is not only a type of dataset or a collection of technologies, but may also incorporate beliefs about ways in which inferences are or ought to be drawn (see Kitchin's (2014: 2) description of a 'new epistemological approach for making sense of the world.') Suggestions as to what Big Data might be able to achieve and what limits there may be to new forms of empiricism are controversial, within criminology as elsewhere (Kitchin 2014; Chan and Bennett Moses 2016). The concept of Big Data is thus flexible, subject to different interpretations among those who seek to employ data-related technologies for a wide variety of scholarly, commercial or 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 Olesker 2012; Wyllie 2013; Staniforth and Akhgar 2015). Yet, as Crawford (2014) points out, Big Data also generates anxieties for the 'surveillers', the security agents that hope to use such

*Janet Chan, UNSW Law, UNSW Australia, Sydney NSW 2052, Australia, and Data to Decisions Cooperative Research Centre; j.chan@unsw.edu.au; Lyria Bennett Moses, UNSW Law and Data to Decisions Cooperative Research Centre.

technology for improving effectiveness. One of these anxieties is 'that no matter how much data they have, it is always incomplete, and the sheer volume can overwhelm the critical signals in a fog of possible correlations' (Crawford 2014). In examining ideas about the use of Big Data for law enforcement and security intelligence, it is necessary to understand the ways in which those involved in operational matters, technology design and policy development understand the term as well as their expectations as to what it can contribute to security outcomes.

This article explores 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). The analysis builds 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 reveals the expectations and anxieties regarding Big Data among stakeholders and concludes that there should be more open public engagement around these issues and that the community should take a more active role in understanding Big Data and influencing the governance of its usage.

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.

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 (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.[1] *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.

Technological frames and sensemaking

The notion of 'technological frames'[2] (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 (iii) technology in use. The authors found incongruence in all three domains between the users and the technologists; these incongruences had led to unanticipated outcomes and unrealised expectations (Orlikowski and Gash 1994: 198).

[1]We combine this with Chandler's (2015) discussion of 'real-time' analysis of data.

[2]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).

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. The introduction of new technology is 'the beginning of a "technological drama" (Manning 1992, 1996) of normalization, adjustment, reconstitution and reintegration' (Chan 2003: 673). 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.

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) 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) and technical expertise can be a form of cultural capital (Chan 2003). Technological change is, however, a double-edged sword, potentially creating problems and constraints for policing, such as leading to greater internal and external demands for information (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).

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 labour, 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). 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).

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 technological change are complex and do not always produce expected improvements (Koper *et al.* 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)

was more rhetorical than real (Sanders, Weston and Schott 2015: 711). In line with previous research on the 'poorly understood and appreciated' role of crime analysts (Cope 2004), the lack of knowledge and training about crime analysis on the part of police managers and officers had meant that new technologies were 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.

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[3] conducted with 38 stakeholders including law enforcement and intelligence officials, oversight agency officers, policymakers, computer technologists and officers in relevant civil society organisations in Australia. The research team worked with various government agencies and the D2D CRC's partners to identify potential interviewees. Twenty-four of the interviews were recorded with the consent of the research participants and verbatim transcripts prepared. For the rest, 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.

Among the 38 participants, 19 were from operational, 7 from technical and 12 from policy organisations (including oversight agencies). 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, despite our requests, mainly in managerial or higher positions.

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 *Making Sense of Big Data for Security*, 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.

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

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 *et al.* 2013). Before asking questions about Big Data, we sought to understand how security agents *normally* use data. 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 (Chan 2003; Sanders *et al.* 2015), 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. … we use any data that we can get our hands on lawfully, certainly, *to assist in our investigation*. (O, emphasis added)

As Crawford and Hutchinson (2015: 11) observe, 'projects of security seek to offer assurances about *the future* and generate expectations that people can count on'. Nevertheless, in terms of the *temporal scale* (Valverde 2014) of their security projects, research participants from operational organisations nominated a range of past-focused, future-oriented, and 'real time' operational purposes for 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 risks (3), policy or service decisions (3), trust building (1) and identification of trends (1). Data could also be used in 'real time' for monitoring current events such as protests (1), human source (informant) management during investigations (1) and situational awareness (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 … can we better analyse it to see what we missed, what we could have done better … the third one was creating the bigger picture … 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* … (O, emphasis added)

In some circumstances, there may be a decision to make around the appropriate response to particular information about a threat from prosecution (in relation to a past event) to disruption (of a potential future event):

> 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*. … We deal very much in shades of grey. Jail may be the best national security outcome …. 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 … 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. 'Real time' activities, with the possible exceptions of situational awareness and events monitoring which can relate to aggregates, also involved individuals (a specific investigation with a human source or services provided to a particular individual based on information about them). All such activities involved security agencies as central actors (cf Chandler 2015). 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. Only one research participant mentioned identified trend analysis as a purpose for which data was used (giving examples of trends in encryption and software use, and crime location). A general focus on individuals rather than aggregates is consistent with the fact that almost all research participants were only interested in *identified*, rather than *de-identified* data, with the use of de-identified data to predict trends a future possibility or rare practice only:

> 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. (O)
> It's no value if it's de-identified. (O)
> It is possible that, in the future, police could use our data to predict trends....(O)

This is also 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 most security agents, a key dimension of their habitus, even at the managerial level.

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. This provides a crucial lens for understanding their expectations of Big Data (*Expectations Regarding Big Data*) and their assessment of benefits and risks (*Winners and Losers in Technological Change*) since those will be framed within the context of

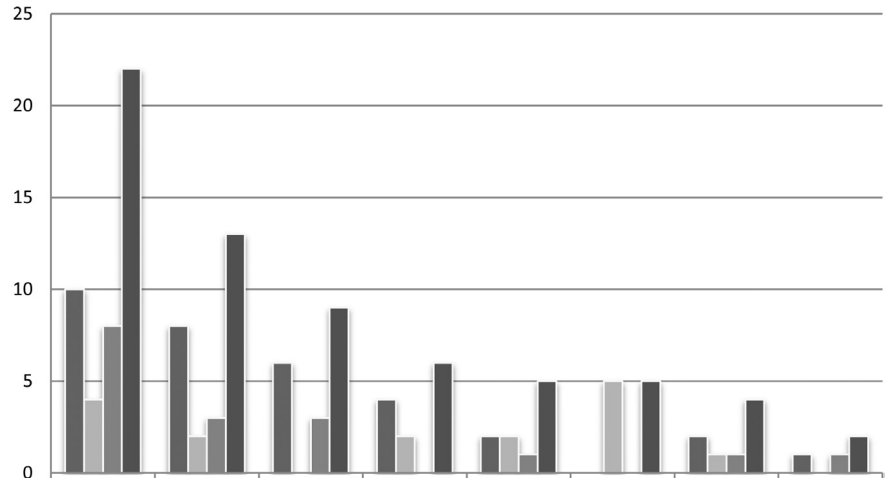
participants' own conceptions of Big Data, both in terms of its meaning and its capabilities. It also brings out differences between existing purposes to which data is currently put (*The Purpose of Data*) and possibilities envisaged within new technologies.

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 arising from academic or other literature, 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.

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)



	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

FIG. 1 Conception of Big Data by type of organisation employing participants ($n = 38$).
*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

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 'find much more complicated, complex relationships—it's this unlock the secret that's within the data' (O), as its defining feature.

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... 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 and the elimination of 'silos'. The majority of these worked in operational organisations:

So Big Data is everything — because I actually consider what we hold, [in] 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 ... 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. (O)

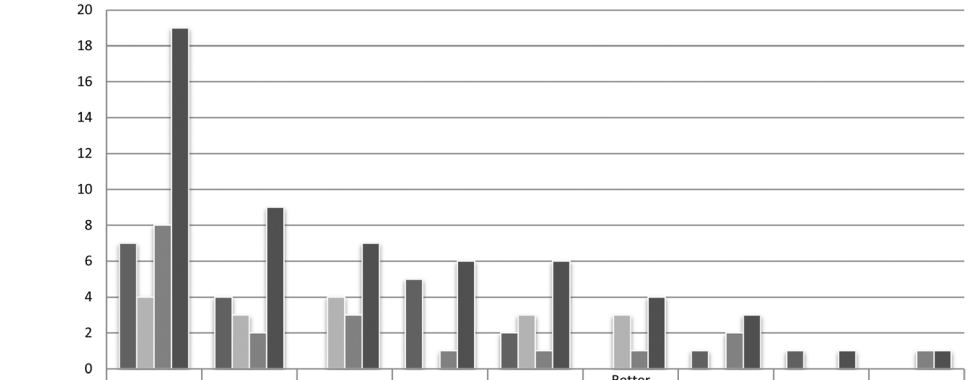
Thus Big Data can generate diverse meanings among those working on or formulating policies for security projects. As well as the obvious question of size, the term captures ideas about analytic capacity, the integration of data sets, the technological horizon and buzz word scepticism. While data analysis was frequently mentioned, research participants did not explicitly associate the term with a different approach to epistemology (cf Kitchin 2014).

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).

Half of the participants referred to Big Data's more advanced analytic capacity, particularly in the context of prediction, network analysis and enhanced insight ('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:



	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

FIG. 2 Perceived capability and value of big data by type of organisation ($n = 38$).
*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

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. (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. … 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. … [T]hat actually gives you a greater level of understanding about somebody before you actually approach them. … 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 three from the policy group mentioned proactive/preventative policing as an opportunity that Big Data could open up for law enforcement and security intelligence:

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)

These statements, including the use of 'indicators' and strategic resource allocation, suggest a pattern- or trend-based approach to policing. As noted above, only one participant in an operational organisation mentioned this as a purpose for which data was *normally* employed. 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 generally focused on 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 *The Purpose of Data* that an important dimension of the habitus of security agents was their shared assumption that data generally (not just Big Data) was used primarily for case-by-case investigative or disruptive purposes. This raises another question about their habitus: what do security agents expect from Big Data technology? This is examined in the next Section.

Expectations Regarding Big Data

Our interviews with operational participants suggest that security agents have diverse expectations about what Big Data will bring. These expectations relate to their *own* conceptions of Big Data, rather than necessarily to any academic or publicly accepted definition. Since more than half of the participants had not been using Big Data in their work (again within their own understanding of that term), growing public awareness about the idea and capabilities of Big Data has created a 'occasion' for a new focus for sensemaking. 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 … 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 … … 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… (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)
>
> 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)

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. In this way, the concerns about a 'mismatch of expectation' (T, from above), may have reduced over time as sensemaking adjusts over time.

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, or better IT resourcing (e.g., through mobile access and faster speeds). 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, which may foreshadow an evolution of technological frames within security agencies. 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.

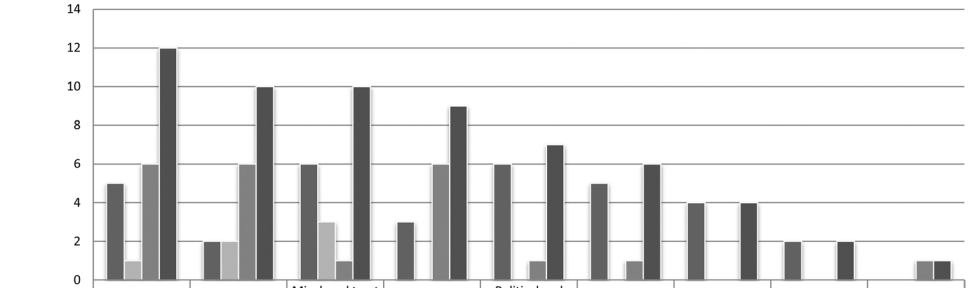
Winners and Losers in Technological Change

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. New data-driven technologies are likely to be taken up to varying 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 and related 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 … (O)
>
> … 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 *Making Sense of Big Data for Security*, 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



	Privacy	Misuse of data	Misplaced trust in technology/ algorithms	Data security	Political and reputational risks	Public perceptions	Overload	Data integrity	Discrimination
Operational	5	2	6	3	6	5	4	2	0
Technical	1	2	3	0	0	0	0	0	0
Policy	6	6	1	6	1	1	0	0	1
Total	12	10	10	9	7	6	4	2	1

FIG 3 Risks of using big data by research participant organisation ($n = 38$).
*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

they vary by the type of organisation participants worked in. 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, 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 or reputational risks, lower public trust and information overload) compared with 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).

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. … 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 ('liable in the public sphere that you knew the risk and you did nothing with it'—O), they made use of data that 'society didn't think they had access to' (T), or they acted on a 'false positive' ('catching totally innocent people'—P):

While anxieties about risks to agencies dominated among operational participants, all categories of research participants identified risks that are more general. 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 or 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. Further, different groups tended to focus on different types of risk, suggesting that enhanced dialogue could facilitate understanding within agencies of public concerns.

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). There are diverse ideas about what the term may mean, what new capabilities may be associated with it and how it may be used in the future. Less than half of the security agents who participated in the research reported that Big Data (using their own understanding of that term) was being used in their unit; their sensemaking around Big Data was therefore not necessarily based on experience with any particular types of datasets or technologies. 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 past-focused activities (e.g. detection and investigation), future-oriented exercises (e.g. prevention, disruption or risk reduction), as well as 'real time' operations (e.g. situational awareness, monitoring of events), 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. In many ways, security agents were still searching in the dark, not totally sure how Big Data was going to help them, except for this sense that 'more data is better' which is not necessarily the case as 'wanting everything' (n = all, without proper filtering tools) is likely to create anxieties about data 'black holes' and information overload (Crawford 2014).

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, as well as better real-time monitoring capabilities, 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). Concerns about high expectations of automation may be less of a problem than basic assumptions about policing approach.

There are many potential futures for greater use of Big Data and data-driven decision support systems 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. 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. 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. For example, while there was an awareness within operational organisations of the limits of fully automated decision-making, there was also a strong sense that algorithms could 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.

Absent from our study is a major group of stakeholders, the general public. Chandler (2015: 6, 11) has discussed the 'empowering potential of Big Data as a way of democratising or redistributing and diversifying power and knowledge' as well as 'changing social behaviour by greater adaptive reflexivity'. As subjects of surveillance, the general population has not caught up with the potential benefits of Big Data, nor a clear appreciation of its risks (see Michael and Lupton 2016). The data being collected and analysed by security agencies is being used internally, not reflected back to the data-subjects to enhance self-governance (cf MOPAC 2016).

While arguments about privacy are familiar (although subject to disagreement), other risks and benefits have been relatively unexplored. As Big Data technology's presence in our lives continues to grow, it is important for us to step up and take a more active role in understanding the prospects and limits of this technology for providing security among our communities and localities. As owners and producers of the majority of Big Data, we need to make more of an effort to influence its governance and regulation. This is particularly important given the diversity of technological frames, including in relation to expectations and risks, even among stakeholder participants in a small-scale study. 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' (see also Harcourt's (2015: 126) observation that surveillance works best 'when it is absent-mindedly forgotten') should alert us to the possibility of the 'securitisation' of Big Data going down the same path, either through ignorance or apathy.

Despite the claims made by proponents of Big Data, there are open questions about its usefulness in criminology and criminal justice (Chan and Bennett Moses 2016). Understanding the potential impact of Big Data in these fields will require an understanding of the different technological frames of security agents, designers and policymakers and, ultimately, the broader public.

Funding

This work was supported by the Data to Decisions Cooperative Research Centre (D2D CRC) through Grant DC52001.

Acknowledgements

The authors would like to thank the whole CRC Law and Policy Program research team for contributing to the project design, and especially Professor Louis de Koker and Dr Alana Maurushat for contributing to 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 responding to our invitations and Gavin Smith UNSW Law colleagues who attended our seminar and two anonymous reviewers for their valuable comments on earlier versions of this article. The views expressed in this article 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.

Chandler, D. (2015) 'A World Without Causation: Big Data and the Coming of Age of Posthumanism' *Millennium: Journal of International Studies*, 2015: 1–19.

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

Crawford, A. and Hutchinson, S. (2015) 'Mapping the Contours of "Everyday Security": Time, Space and Emotion', *British Journal of Criminology*. doi:10.1093/bjc/azv121

Crawford, K. (2014) 'The Anxieties of Big Data', *The New Inquiry*, 30 May 2014.

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: 977–96.

Harcourt, B. (2015), *Exposed: Desire and Disobedience in the Digital Age*. Harvard University Press.

Kitchin, R. (2014), 'Big Data, New Epistemologies and Paradigm Shifts', *Big Data and Society*, 1: 1–12.

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: 212–21.

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*, 2501–13. 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: 10–20.

Michael, M. and Lupton, D. (2016), 'Toward a manifesto for the "public understanding of big data", *Public Understanding of Science*, 25: 104–116.

MOPAC (2016), *Crime Dashboard* (website), available online at https://www.london.gov.uk/WHAT-WE-DO/mayors-office-policing-and-crime-mopac/data-and-research/crime/crime-dashboard (last accessed 20 May 2016).

Nogala, D. (1995), 'The Future Role of Technology in Policing', in J. P. Brodeur, ed., *Comparisons in Policing: An International Perspective*, 191–210. 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: 711–29.

Sheptycki, J. (2004), 'Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of intelligence-led policing', *European Journal of Criminology*, 1: 307–32.

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*. 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/.