University of New South Wales Law Research Series

CAN "BIG DATA" ANALYTICS PREDICT POLICING PRACTICE?

JANET CHAN AND LYRIA BENNETT MOSES

[2020] *UNSWLRS* 82

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Paper for
Workshop on *Constructing, Predicting and Experiencing Risks: Crime, Risk and Technology*, 15-16 June 2016, Wilfred Laurier University, Brantford, Ontario

Can "Big Data" Analytics Predict Policing Practice?

Janet Chan and Lyria Bennett Moses
Faculty of Law, UNSW Australia and Data to Decisions Cooperative Research Centre[1]

Final version published as Chan J and Bennett Moses, L, 'Can Big Data Analytics Predict Policing Practice' in Hannem et al. (eds) Security and Risk Technologies in Criminal Justice (Canadian Scholars Press 2019)

Abstract
Predictive policing—the use of data, combined with mathematical or machine learning algorithms to predict the risks of crime in specific locations and times—has raised hopes as well as strengthened the rhetoric of using technology for crime control. The apparently enthusiastic uptake of predictive policing software in the US and elsewhere, together with the hype of "Big Data", has created a new orthodoxy that technology can make policing "smarter" and "information-based" rather than subject to human bias and occupational habits. By reviewing past and current research on the use of technology and innovation by police, this paper develops a framework for conceptualising factors that affect the uptake of predictive policing and processes that influence its impact on police practice.

1. Introduction

In *Policing the Risk Society*, Ericson and Haggerty (1997:3) have offered a "fundamental reassessment of how we think about police". Writing in the late 1990s, Ericson and Haggerty conceptualised police as "knowledge workers" in the "risk society" (Beck 1992). Rather than seeing policing only as "what the public police do", the authors argue that "policing consists of the public police coordinating their activities with policing agents in all other institutions to provide a society-wide basis for risk management (governance) and security (guarantee against loss)". Police mobilisation is therefore "not only a matter of intervention in the lives of individual citizens but also a response to institutional demands for knowledge of risk" (1997:5). Ericson and Haggerty (1997:114) have identified two technological inventions that "have made a profound contribution to the constituting of risk society": statistical thinking and communication technology:

> Statistics and probability theory, constituted in computer formats, structure truth. They present risk data as the basis of an objective standard that people *must* accept as objective reality and therefore used to form their identities and behavior. Although the risk classifications and categories, and the resultant identities and behaviour, are socially constructed, once in place they are 'relative to nothing'; and become *the* standard (Hacking 1992:135). They become truly rational and drive social change by routinizing it in institutional procedures. (Ericson and Haggerty 1997:115)

The authors suggest that computers "allow the development of new formats of risk communication, as well as instant dispersal of knowledge of risk to interested institutions" (1997:13).

[1] This research is partly funded by the Data to Decisions Cooperative Research Centre (D2D CRC). The views expressed in this paper do not necessarily represent those of the D2D CRC.

The advent of "Big Data" analytics appears to be a continuation or even an escalation of this trend to combine statistical thinking and communication technology to present "risk data". As Chan and Bennett Moses (2016: 23) point out, the term "Big Data" is defined in a variety of ways: "by reference to the size and type of data sets being employed, the capabilities of a data storage, processing and/or analytic system, as a set of marketing claims about what is enabled by particular technologies or as a social and cultural phenomenon". While there are many potential uses of Big Data technology to policing (e.g. the automation of intelligence gathering through social media analysis), an important application of data analytics is the use of computer modelling or algorithms as predictive tools for risk analysis or crime prevention.

The rise of "predictive policing" goes beyond hotspot analysis, problem-oriented policing and crime mapping to use data and analytics to "forecast where and when the next crime or series of crimes will take place" (Uchida, 2013: 3871). These predictions can be about "places and times with an increased risk of crime", "individuals at risk of offending in the future", creating "profiles that accurately match likely offenders with specific past crimes" or identifying groups or individuals at risk of becoming victims of crime (Perry et al., 2013: 8–9). In addition to forecasting, predictive policing involves taking a proactive response to crime where the goal is to "change outcomes" (Beck and McCue 2009) through the identification of "crime prevention tactics/strategies", mostly changes to police deployments, and the evaluation of police programs (Wilson 2009).

The apparently enthusiastic uptake of predictive policing software in the US and elsewhere, together with the hype of "Big Data", has created a new orthodoxy that technology can make policing "smarter" and "information-based" rather than subject to human bias and occupational habits.

This paper will focus on the following research question: will the introduction of predictive policing (Uchida 2014), especially in the environment of Big Data, change policing practice fundamentally? Given the limited availability of independent evaluations of predictive policing, the paper will review past and current research on the use of technology or innovation by police and develop a framework for conceptualising factors that affect the uptake of predictive policing and processes that influence its impact on policing practice.[2]

The argument of the paper will unfold as follows. Section 2 describes the attractions of data analytics for policing, the state of current development, and the extent to which it has been taken up by police organisations. In order to answer the research question posed, Section 3 develops a conceptual framework for analysing the diffusion, uptake, and impact of policing technology. This framework draws on organisation and policy studies, and empirical research on past instances of policing innovations. Section 4 assesses the likely uptake and impact on policing practice of predictive policing using current knowledge about predictive policing, and empirical research in Australia. Section 5 summarises the analysis and discusses its theoretical and practical implications.

2. Predictive Policing Technology

"Predictive policing" is a term applied to a range of analytic tools and law enforcement practices. What links these together is the claimed ability to "forecast where and when the next crime or series of crimes will take place" (Uchida 2013: 3871), combined with changes in law enforcement decision-

[2] Note that the focus of this paper, as with most research on policing innovation, is on public police rather than the private policing sector. While elements of our model, especially in relation to technical and discursive elements, are likely to be equally relevant in the private sector, the political/legitimacy issues will not necessarily be as influential.

making, particularly deployment of officers, based on those forecasts. As practised, mostly within the United States but also elsewhere, the analytic element typically involves an off-the-shelf or adapted software tool that analyses historic crime data (and sometimes other data such as social media, weather, mortgage defaults) to predict most commonly where, but sometimes by whom or to whom, crime will take place in the future.

Software used for predictive policing can range from simple spreadsheet programs to complex algorithms. It can be open-sourced or inexpensive (Olesker 2012), purposed off the shelf, or specially tailored. Information on the tools themselves is often limited and source code is often a trade secret. This makes it difficult to evaluate products provided by organisations such as IBM® (e.g., Blue CRUSH in Memphis and Blue PALMS in Miami), Information Builders® (Law Enforcement Analytics), Azavea® (HunchLab), SPADAC® (Signature Analyst®), Accenture® and Hitachi®. There is some information about PredPol®, in that it is based on published research work centered at UCLA and Santa Clara University using an earthquake prediction model involving a self-excited point process (Mohler et al 2011). Essentially, rates of crime at a particular location were based on background factors as well as the "near repeat" (or aftershock) events related to historic events nearby in time and space. Outputs are 500 square foot areas where it is predicted crime is more likely to occur. Police are then assigned to focus patrols on those areas. Other products rely on different models which build in demographic data, rates of home foreclosures, weather patterns, geographic features and social media analysis.

As a phenomenon, predictive policing is more than a set of tools or the ways in which they are used within particular police departments. It also relies on a belief that the use of these tools in particular ways is effective in reducing crime. More specifically, predictive policing is premised on the assumptions that it is possible to use technology to predict the likelihood of crime before it happens (van Brakel and De Hert 2011), that forecasting tools can predict accurately, and that police will use this knowledge effectively.

An increasing number of police organisations are reported as using predictive policing tools, mostly to predict future areas where the likely frequency of future crime is higher. Focusing solely on tools that are explicitly forward-looking or "predictive", media searches revealed the adoption of predictive policing software and approaches in the following jurisdictions:

> Asia: Delhi, India (Enterprise Information Integration Solution); China (Situation-Aware Public Security Evaluation (SAPE) platform)
>
> Europe: Milan, Italy (KeyCrime), Birmingham UK (Accenture), Kent UK (PredPol), Manchester UK (PredPol, SPSS/IBM), London UK (Accenture, PredPol), Northern Ireland UK (IBM)
>
> North America: Albuquerque NM, Alhambra CA (PredPol), Atlanta GA (PredPol), Charleston SC (SPSS/IBM), Charlotte-Mecklenburg NC (Information Builders Law Enforcement Analytics), Chicago IL (Predictive Analytics Group), Dallas TX (for financial crimes), Detroit MI (Datameer), Fort Lauderdale FL (IBM), Illinois State Police (Riverglass), Indio CA (Smart Policing Initiative), Kansas City KS (Information Builders Law Enforcement Analytics), Los Angeles CA (PredPol), Macon GA (SPSS/IBM gun crime only), Memphis TN (IBM Blue CRUSH), Miami FL (IBM Blue PALMS), Minneapolis MN (IBM, MPD Crime Analysis Unit), Modesto CA (PredPol), New York City NY (HunchLab), Norcross GA (PredPol), Richmond VA, Santa Cruz CA (PredPol introduced 1 July 2011), Seattle WA (PredPol), Shreveport (funded by NIJ)
>
> South America: Sao Paulo, Brazil (Microsoft Detecta rolled out in January 2015)

The underlying model of predictive policing is described in Perry *et al.* (2013: 128). As they state, predictive policing is "not fundamentally about making crime-related predictions" but about implementing a prediction-led policing business *process*, which consists of a cycle of activities and decision points: data collection, analysis, police operations, criminal response, and back to data collection. Each stage of the cycle involves choices that are made under diverse organisational conditions. For example, choices must be made as to what types of data to collect and how frequently to collect it and data analysis may be carried out in house (with greater or fewer human and financial resources) or using a standard software package (Perry *et al.* 2013).

The term "predictive policing" enters the fray amidst a variety of other related but distinct terms describing policing approaches and styles. For example, it is clearly a type of "intelligence-led" policing (Maguire 2000: 315) and data-driven policing. It is consistent with a temporal shift from post-crime to pre-crime and pre-emptive approaches in policing (Zedner 2007; van Brakel and De Hert 2011) and shift in focus from punishment for moral failings to risk management and loss-prevention rather than punishment for moral failings (Zedner 2007, Ericson and Haggerty 1997). Particularly where it focuses on the location of future crime, it is closely related to "hot spot" policing (Sherman et al 1989), except that it explicitly models the likely future locations of "hot spots", often through evidence of statistically broader geographical impact of a single crime event (e.g., Bowers et al. 2004). Some police activities, such as monitoring social media feeds in real time during large events or automatically analyzing video feeds from CCTV cameras to detect criminal activity, may be part of a predictive approach to policing or may be used as a form of situational awareness as to the present.

3. Understanding the Diffusion, Uptake and Impact of Technology in Policing

While research on the diffusion, uptake and impact of technology on policing is scarce (Manning 2014) there are a number of studies on the uptake and impact of policing *innovation* (see Wills and Mastrofski 2011) such as problem-oriented policing (Weisburd et al. 2010), hot-spots policing (Braga et al. 2014), intelligence-led policing (Darroch and Mazerolle 2012, Sanders et al. 2015) and community policing (Graziano et al. 2014, Chan 1997). These studies can inform our development of a framework for understanding why certain technology is adopted and what impact does the technology have policing practices. Predictive policing is in fact an innovation in *process*, or as Perry et al. (2013:128) call it, a "prediction-led policing process".

We will continue to use the term "technology" in this paper given the dependence of data analytics on technological advances such as the speed and capacity of data collection and data storage in relation to predictive policing processes. Nevertheless, technology needs to be conceptualised more broadly as consisting of three dimensions: (i) the *technical*, as already mentioned, (ii) the *symbolic*, the ideological or discursive representation of how the technology is promoted, especially its narrative of being scientific and innovative, and (iii) the *organisational*, the institutional or group interests that are at stake in the uptake of this technology (see Feldman and Orlikowski 2011; Chan 1992; Elmore 1978; Allison 1971). For example, in predictive policing, the "marketing" or hype of this technology (the discursive dimension) and the potential interests of policing agencies in enhancing efficiency and effectiveness (the organisational dimension) have been as important as, if not more important than, its actual technological capabilities.

Uptake and Impact of Technology

Two key elements in the framework we are developing in this section also require more discussion. The first is the *uptake* or adoption of technology and the second the *impact* of technology. As studies

in social studies of technology show, the uptake or adoption of technological innovations is never an all-or-nothing concept. There are various degrees of uptake: acceptance of the ideas underlying the technology, decision by leaders of organisations to invest in it, purchase of equipment or software associated with it, piloting of the technology in parts of the organisation, or full-blown adoption of the technology throughout the organisation..

Once taken up (to whatever degree), the technology has to be implemented before it can have impact on practice. The importance of implementation cannot be overstated, and this will be discussed below. A more immediate concern is how impact is defined and detected. An important concept in this paper is the notion of "practice", which is central to our understanding of how technology makes an impact (see Chan 2003, Feldman and Orlikowski 2011, and more generally practice theorist such as Bourdieu, Giddens and Schatzki). Assessing the impact of a new technology requires an appreciation that "technology is not valuable, meaningful, or consequential by itself; it only becomes so when people actually engage with it in practice" (Feldman and Orlikowski 2011:1246). Technology as used in practice can be quite different from the "strategic design" and anticipated uses of managers and technologists; applications and consequences may be unintended and unexpected (Feldman and Orlikowski 2011:1146). Organisational outcomes, or the impact of innovation, is shaped more by "the specific technologies in practice (enacted technology structures) that are recurrently produced in everyday action" than by the technological tools themselves or by hypothesized or general uses (Feldman and Orlikowski 2011:1147). Technology in practice is recursive – over time, particular uses draw on past experiences, including past uses (Feldman and Orlikowski 2011:1247?). Users learn to "make sense" of new technologies through a combination of organisational instruction and training, their own experimentation and encounters with a tool's possibilities and limits and their own reading of the discourse surrounding the technology, both within and outside their organisation. Thus, institutional, interpretive and technological conditions affect the extent and manner of use (Feldman and Orlikowski 2011), and hence the impact over time. The ultimate impact of predictive policing on police practice is thus not only linked to the number of police departments claiming to adopt this approach or purchasing specific software ("diffusion"), but more importantly to the real effect on police practices, including policing strategies, police deployments, resource allocations, program evaluations and modifications over time ("impact").

A Socio-Technical Framework for Uptake and Impact of Technology

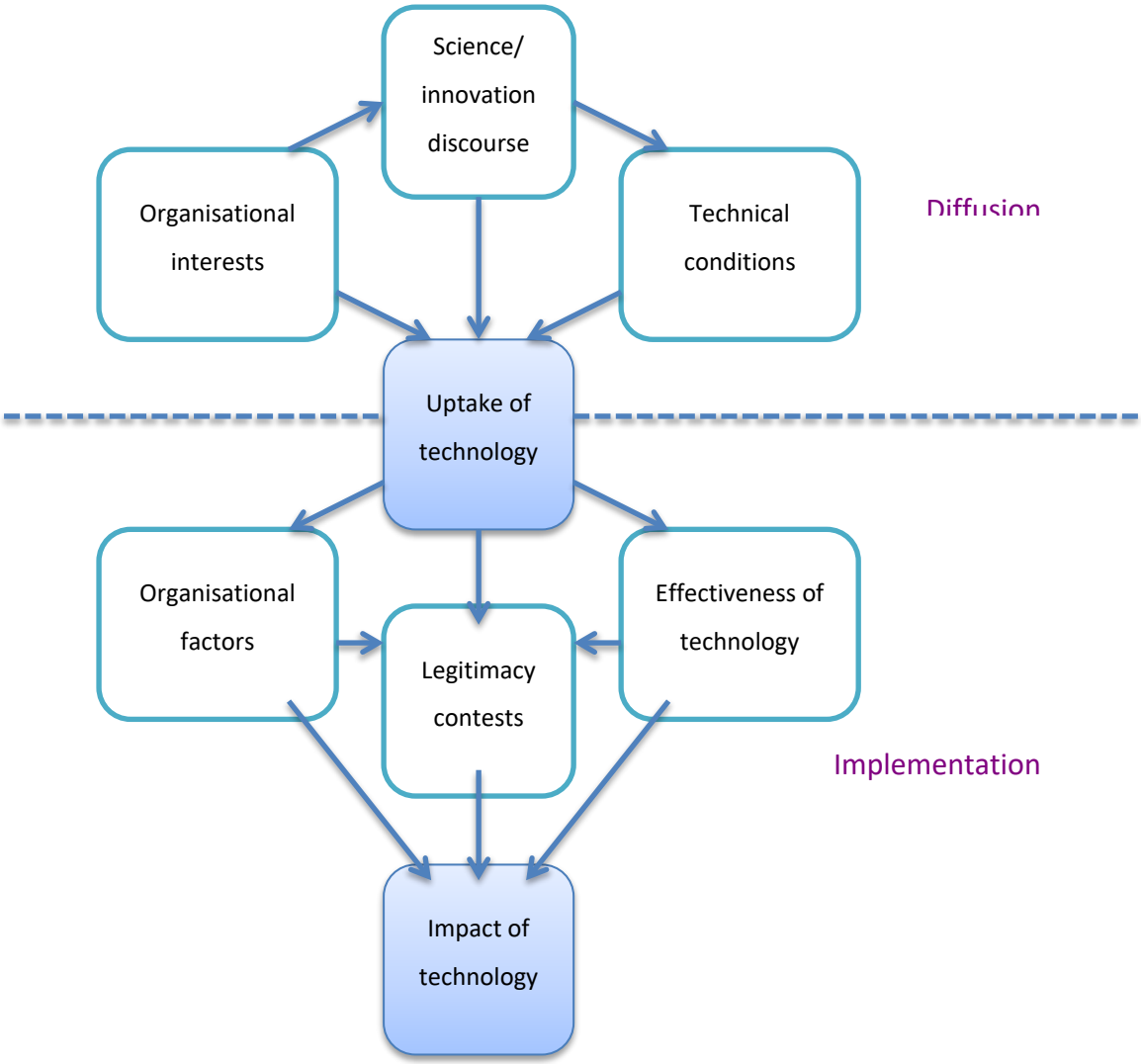
Figure 1 provides a schematic overview of the framework we have developed for understanding factors affecting the uptake and impact of technology. The framework is indicative rather than predictive or deterministic. It captures the social and organisational dynamics at work in the processes of diffusion and implementation of technology.

Focusing on the upper half ("diffusion") of the diagram, it is hypothesised that conditions favourable to the uptake of a particular technology include the *symbolic* significance of using advanced science/innovation for leaders of organisations as a way of gaining prestige, as well as a way of advancing *organisational interests* such as improving effectiveness and efficiency. However, the *technical conditions* have to be favourable for such an uptake, i.e. the technology has to be proven and have credibility for potential users. Here, the focus is the processes leading to a decision, at management level, to implement a predictive policing program, potentially through the purchase of particular software.

Moving to the lower half ("implementation") of the diagram, it is hypothesised that once technology has been "taken up" by an organisation (e.g. decision is taken by management to purchase the equipment/software for the technology), then the impact of technology on practice depends on how

well the technology is accepted and implemented: whether the *technology has proved to be effective* in meeting users' expectations, whether there are *administrative, political or cultural obstacles within the organisation* impeding the effective use of the adopted technology, and whether there are *contests about the legitimacy* of the use of this technology, especially from outside the organisation, e.g. citizen groups, human rights organisations, court challenges, etc.

Figure 1: A Model of Uptake and Impact of Technology



Impact can be unpredictable; there can often be unintended consequences (Feldman and Orlikowski 2011). Conditions favorable to the achieving impact as expected include: that the adopted technology is reliable and effective; that there is a well-managed process of implementation, including adequate training, support and resources; that the adopted technology does not threaten established power structures; that the adopted technology does not require a marked change in users' standard operating procedures or work culture; and that the adopted technology is not politically controversial among citizens or not perceived to lead to undesirable outcomes for the community (or at least specific sections of the community). However, the absence of one or more of these does not imply zero impact. Positive factors may override negative ones, or practices may shift to accommodate the interests of users or citizens.

The distinction between uptake and implementation/ impact can be blurred depending on which level of the organisation we are discussing. For example, though written in terms of the "uptake" of Intelligence-Led Policing (ILP), Darroch and Mazerolle's (2012) research on New Zealand Police NZP) can also be interpreted as a study of implementation/impact at the local level. This is because NZP "began experimenting with ILP from the late 1990s in a small number of areas" but the use of ILP was encouraged, not mandated (2012:7). In one sense, the police organisation has already adopted ILP but has left its implementation to the local leaders.

Support for Framework from Previous Research

While the literature is relatively sparse, the available empirical research on the uptake and implementation/impact of policing innovations (including technology) provides general support for the above framework. For both uptake and impact, the importance of the three dimensions of technology—organisational, symbolic and technical—is highlighted. Note, however, that the three dimensions, though conceptually distinct, are often intertwined in practice. As can be seen in the following discussion, the same feature can impact along multiple dimensions. Further, an impact along one dimension can itself cause an impact along another.

Organisational Dimension

Organisational factors affecting uptake/ implementation/ impact of technology can take many forms, including leadership, management of the introduction of technology, organisational politics, and cultural resistance. Technological change can often destabilise the power balance within an organisation, leading to forms of resistance among operational police (Ericson and Haggerty 1997, Koper et al. 2014). There are also studies, discussed below, demonstrating that there can be a low *fidelity* of implementation (Hassell and Lovell 2015) where users employ tools, designed to change policing practice in fundamental ways, for more traditional purposes (Sanders *et al.* 2015, Chan 2001; Braga and Weisburd 2007; Koper et al. 2014). However, this is contingent on management style and organisational culture (Darroch and Mazerolle 2012).

Hassell and Lovell (2015) have highlighted the importance of looking at *fidelity* of implementation when assessing policing innovations. Fidelity of implementation is "the extent to which a reform, as implemented, matches the way it was originally conceived" (2015:507). Unless an innovation has been implemented according to the original concept, it is impossible to (a) attribute any "success" to the innovation, or (b) conclude that the innovation has "failed". Fidelity of implementation can also help explain *why* a particular innovation fails or succeed. In fact, the feasibility of an innovation/reform can be assessed from examining the fidelity of implementation (507). The five dimensions of fidelity are: "(1) *adherence* to the planned design, (2) *exposure* or *dose* (amount delivered), (3) *quality* of the delivery, (4) *participant responsiveness* and (5) *program differentiation* (presence or absence of the essential elements of the reform/program) (Hasson 2010)" (Hassell and Lovell 2015:508). Their case study in a small US Midwest police department found that "POP has not been institutionalized or implemented in a manner that is consistent with Herman Goldstein"s conceptualization, although the department claimed to have done so" (2015:516). When looking at the impact of an innovation, it is thus important to ask "impact *of what*" – there may be a change in practice that does not correspond to the innovation that was adopted.

In some instances cultural issues and management of innovation issues are intertwined. For example, research in six Canadian police services found that the use of "crime science" and analytic technologies to support intelligence-led policing was more rhetorical than real (Sanders et al. 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 (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, p. 724).

Conversely, Darroch and Mazerolle's (2012) study of the "uptake" of ILP within NZ Police found that the high regard for local intelligence units was an important factor:

> For ILP to succeed, frontline officers needed to hold their local intelligence units in high regard. To ensure this, highly credible sworn officers were sought and trained for intelligence roles. Technical proficiency was demonstrated through skill in the use of information technology tools and consistency in developing quality intelligence products that focused on achieving crime reduction goals. (Darroch and Mazerolle 2012:24)

The use of sworn officers for intelligence role is a strategy related to the *organisational* dimension of implementation, given the lack of trust demonstrated by police against civilian analysts.

Darroch and Mazerolle (2012) found leadership style (transformational rather than transactional) and the encouragement by leaders to be factors associated with "strong uptake" of ILP, although they did not find clarity of goals or manager commitment to ILP to be important factors. In terms of organisational culture, the researchers found an association between "strong uptake" and a "can do" subculture:

> Our research shows the emergence of a distinctive subculture associated with the strong uptake of ILP innovation. The ILP subculture had the following characteristics: a broadly accepted focus on crime reduction as the overarching goal for local police, support for partnerships and problem solving as legitimate policing strategies, tolerance for experimentation and trial of novel approaches, support for ILP, a willingness to follow ILP leadership, openness to learning, and a willingness to participate and contribute to improvement and general innovation. (Darroch and Mazerolle 2012:17-18).

Koper et al. (2014:216) found that the impact of new technology on police could be "complex and contradictory": while technological advances could improve communication across the organisation, they were also potentially detrimental to work relationships and organisational justice:

> Technology can also worsen perceptions of inequality for line-level staff, particularly patrol officers who may feel heavily burdened and scrutinized by the reporting demands and monitoring that often come with new information and surveillance technologies (in-car and body-worn cameras provide examples of the latter). … All of these factors can foster resistance to technology and undermine its potentially positive effects. (2014:216)

The authors concluded that new technology also did not appear to have led to improved management and accountability at the rank-and-file level:

> … Our observations suggest that while technology has fostered accountability at higher managerial levels in policing (e.g. through Compstat-type management processes), the innovative use of technology as a tool by middle and lower-level supervisors to manage the

> performance of line-level officers still is neither institutionalized nor clearly understood. (2014:217)

The limited impact of new technology on police use of technology for strategic purposes was a consistent finding across several studies (Chan 2001; Braga and Weisburd 2007; Koper et al. 2014). Chan's (2001) case study in Australia highlights the role of cultural factors in mediating the impact of technological change. She found a clash in "technological frames" (Orlikowski and Gash 1994) between the users and the architects of the information system: police expected IT to make their work easier without their having to change existing policing or management styles while the architects had intended that police would use the system for tactical and strategic purposes. She found that even though new technology gave police an opportunity to follow a "smarter" or problem-oriented style of policing, traditional policing styles and values still dominated.

Koper et al. (2014:216-217) similarly observed that police use of technology was affected by the way they "frame policing in terms of reactive response to calls for service, reactive arrest to crimes, and adherence to standard operating procedures", so that they were much more likely to "use IT to guide and assist them with traditional enforcement-oriented activities than for more strategic, proactive tasks".

In general, as Braga and Weisburd (2007:17) observe:

> The police most easily adopt innovations that require the least radical departure from their hierarchical paramilitary organizational structures, continue incident-driven and reactive strategies, and maintain police sovereignty over crime issues.

Thus innovations such as "hot spots" policing and "broken windows" policing "appeal to law enforcement practitioners primary because they allow mostly traditional tactics to be deployed in new ways with the promise of considerably greater results", while the police have generally resisted the adoption of community policing and problem oriented policing (Braga and Weisburd 2007:17).

According to Koper et al (2014), the inadequacy of training may have been one of the factors affecting the impact of technology. If the objective is to change the approach to policing, for example, it is not enough to demonstrate "the basics" as to how new software works technically. Training must also include guidance as to "how both the organization and individual officers can benefit from use of the technology" (Koper et al. 2014:217).

Symbolic Dimension

The adoption of technology is not only driven by technological advancements but also by the symbolic significance of using new technology. The "scientisation of police work", as Ericson and Shearing (1986:134) point out, provides a "veil of legitimacy over police work". Technological innovations can also bring prestige to police organisations that adopt them. Adjectives associated with data-driven approaches to decision-making (such as "smart" analytics) reflect positively on those who employ them.

Where technology presents broader risks to the community (or subsets thereof), this can change the discourse around that technology. Chan (2003:674) gives some examples of the kinds of risks that information technology can bring:

> … information technology can create new risks such as illegal or unauthorised use of information (Chan et al. 2001:112), the spreading of inaccurate or misleading information (HMIC 2000; Ericson and Shearing 1986:144), and the unfair targeting of specific groups based on "categorical suspicion" (Marx 1988; Meehan and Ponder 2002).

The use of new technology is also likely to raise concerns about surveillance, privacy, profiling, algorithmic accountability and "function creep". Such concerns can escalate into contests about the technology's legitimacy. Because we are focusing on impact, we do not analyse justifications for such concerns here, rather the focus is on the effect they may have on the uptake of predictive policing technology.

Technical Dimension

The importance of the technological dimension itself to both adoption and impact is often taken for granted. Clearly, technology will only be adopted if its function corresponds to a perceived organisational need or objective. Management will also need to be persuaded that it has been proven to be, or is at least likely to be, effective in performing its function. After adoption, effectiveness and ease of use are important in building user trust and confidence. Once adopted, technology can quickly lose its gloss if it fails to live up to its promise, either through technical problems or failure of implementation. Koper et al. (2014) found that technical problems during the implementation of new technology can complicate some of the cultural problems. As they write: "implementation experiences and functionality problems with new technology have important ramifications for the acceptance, uses, and impacts of that technology" (2014:215-216). In their study, difficulties experienced by one agency stemming from technical problems and user interfaces that officers found difficult and cumbersome to use and the need to learn new offence codes had subsequent negative effects on officer attitudes and performance. Implementation issues may be minimised where there is greater consultation around requirements at the adoption stage and sufficient technical assistance and training at the implementation stage (2014: 216).

4. Likely Uptake and Impact of Predictive Policing Technology

The framework developed in Section 3 can help us assess the likely uptake and impact of predictive policing technology. A number of unique features in predictive policing may set this innovation apart from previous technologies. In general, many conditions favourable to the uptake of this technology by police organisations are present. However, the impact may be less than anticipated.

In exploring the likely uptake and impact of predictive policing, we rely on technical and policing studies literature as well as qualitative analysis of interviews conducted with law enforcement and security intelligence officials as part of a broader project[3] exploring the use of Big Data and data analytics for national security. In interviews we asked a series of broad questions about data practices

[3] This project received human research ethics approval from both UNSW Australia (Approval number 14 168) and from Deakin University (Approval number 2014-295) in December 2014. To assist in recruiting Australian participants, the Secretary of the Australian Attorney-General's Department assisted by sending letters to the relevant agency heads endorsing the research project and suggesting that they encourage their staff to participate in the project when invited. Of the 38 participants interviewed in Australia, 11 were from law enforcement (LE), 8 Federal and 3 State, 5 were from security intelligence agencies (INTEL) and 2 were from a federal agency that provides support for federal and state law enforcement. Although the law enforcement views are obviously the most pertinent here, there are some important observations that have been included despite coming from other parts of the broader security community. In particular, intelligence agencies generally had more experience with data-driven decision-support technologies. Some of these had joint operational/policy roles or technical roles.

generally, and attitudes to and uses of Big Data in particular. These questions explored topics including how data is used within their unit, issues around the sharing of data, what data is used for, what particular tools are used, what capabilities they associated with Big Data, what barriers existed to greater use of data analytics generally and Big Data in particular, and what risks were associated with Big Data. Interviews were semi-structured, with opportunity for dialogue between the interviewer and the research participant. The topic of predictive policing was not specifically included as an interview question. The responses should thus not be interpreted as confirming or denying the use of particular technologies or practices associated with predictive policing. Nevertheless, they provide a broad gauge to understand organisational understandings of and approaches to data analytic tools more generally.

A notable finding is the practices and technologies of predictive policing were not explicitly mentioned by participants from operational organisations, even when prompted about their uses of data and Big Data tools. In addition, specific predictive policing software (as opposed to general analytic tools) were not mentioned in the interviews when we asked participants to describe the tools they used. However, there were references to related practices such as identifying "hotspots" (ID removed), the capacity of Big Data to provide "a more complete picture of exactly what's going on" (ID removed) and the use of data generally for crime prevention (ID removed) and deployment (ID removed). Some participants reported use of geospatial or location-based analytical tools, including Geofeedia®, a location-based intelligence platform for social media analysis, and esri®. It remains possible that predictive policing is being used in Australia; we did not conduct interviews with all law enforcement agencies, and sample sizes are small. Nevertheless, the practices around predictive policing seem not to be widespread in Australia. There are, nevertheless, uses of Big Data analytics including the use of the Australian Crime Commission National Criminal Intelligence Fusion Capacity to identify "previously unknown criminal threats to the Australian community" (Australian Crime Commission 2013).

Table 1 summarises the factors that are likely to affect the uptake of predictive policing and impact on policing practices in Australia. Each of the factors can have positive (indicated by +), negative (-), mixed (+/-) or unknown (?) effect on uptake or impact. Note that each factor can relate to one or more dimensions (technical, organisational and symbolic) discussed in the framework in Figure 1.

Table 1: Factors Likely to Affect Uptake and Impact of Predictive Policing in Australia

FACTOR	UPTAKE			IMPACT		
	Organisational	**Symbolic**	**Technical**	**Organisational**	**Symbolic**	**Technical**
Effectiveness		+	-		-?	-?
Cost	+/-		-	+		
Human resources	-?			+/- (*)		-?
Training				-?		-?
Comprehensive outputs			+			+
Complex/opaque			-?	-	-	-
Infrastructure	-		+	+		+
Location-focus	+/-			+/-		
Data – inaccuracy				-	-	-
Data – sharing			- limit options			-
Data – increased access	+				-	
Data – non-individualised				-		
Centralisation	+			-		+
Discourse – smart	+		+	+		-
Discourse – pre-crime/risk	+ over time					
Discourse – crime control	+			+		
Discourse – dystopian					-	
Discourse – neutrality	+	+		-	+	
Discourse – discriminatory impacts					-	
Technological momentum	+					

* Generation may impact on whether the impact is positive or negative.

Effectiveness

The media discourse around predictive policing suggests that it is highly effective. Percentage reductions in crime have been reported across the jurisdictions employing predictive policing software tools (e.g., Turner et al. 2014, Mitchell 2013, Olesker 2012, Ibrahim 2013). However, these are not backed up by evidence or references.

In Bennett Moses and Chan (unpublished), we have explored limitations of predictive policing software and approaches, we point out that they are based on several assumptions that may not always hold. There are issues of data collection, in particular the limited extent to which "reality" is captured in police-held crime data. There are issues of data analysis including the presumption of continuity (which assumes no relevant intervention), choice of variables, technical bias in algorithms, and the frequent assumption that location is key to predicting crime. There are also assumptions about police operations, including the focus on police deployments as the primary intervention Finally, there are questions of criminal response and the impact that police deployments have on preventing crime. While these are not analysed here, they do combine to suggest that the effectiveness of predictive policing as a security strategy is not guaranteed and can thus only be measured through evaluation.

Hunt et al.'s (2014) evaluation of a 2011 predictive policing experiment in Shreveport Police Department in Louisiana found that there was no statistical difference in crime rates between the experimental (predictive policing) and the control districts. The effectiveness of predictive policing has yet to be demonstrated.

But Hunt et al (2014) is not evidence that predictive policing is an ineffective strategy either. The "null effect" was explained in terms of three factors: the low statistical power of the tests; a failure of program implementation as there were variations in the extent to which the prevention model was implemented between districts and over time; or a failure of program theory, i.e. the program design was "insufficient to generate crime reduction" (Hunt *et al.* 2014, p. xv). The implementation issues point to a weakness in the management of the innovation:

> …treatment districts did not follow all aspects of the prevention model. Most important, the monthly planning meetings to set and maintain intervention strategies did not occur. These meetings were to be a key mechanism to ensure the prevention strategies were the same across police commands, and consequently to increase the statistical power needed for the impact analysis. Instead, the experimental districts made intervention-related decisions largely on their own … the strategies and levels of effort employed varied widely by district and over time. (Hunt *et al.*'s 2014, p. xiii)

There are thus reasons to doubt that predictive policing will be effective in reducing crime, but until properly implemented and evaluated, it is difficult to tell.

Cost

Whichever software is deployed for predictive policing, there are financial costs involved. Money will need to be spent either on licensing specialist software or hiring data analysts to work with more basic tools. The financial cost itself is a potential barrier to the use of predictive policing. As one participant (with a joint operational/technical role) from a state police force (ID removed) stated: "[Data analytics] is outside our role. We don't have the resources." However, tight budgets can also be used to justify innovation (to enhance efficiency) and can increase managerial support for use of a product once it is purchased in order to justify the initial investment.

Human resources

Human resources are problematic even if the budget exists. A research participant (ID removed) who is a manager in federal law enforcement referred to the short supply of analysts "across the national security space". On the other hand, younger generations may be more willing to learn about and adopt computer-based approaches to understanding crime. Given the time taken to gain the experience that is the foundation of instincts, computer tools may be seen as a way for younger police officers to advance. Their greater technological expertise can become a form of cultural capital. This depends on how crime analysts are viewed within organisations, and the extent to which data-driven approaches to policing come to dominate. Sanders et al (2015) have explained how crime analysts often have a lower status within law enforcement agencies. However, the possibility of becoming "data scientists" in line with what has been described by Harvard Business Review as the "sexiest job of the 21st Century" (Davenport and Patil 2012) may change attitudes of those considering such a career, and those working in law enforcement more generally. This may, on the other hand, leave older, more established police officers feeling left behind by technology.

Training

Training for new systems can raise issues at the implementation stage. One participant (ID removed) from a state police force pointed out general deficiencies in training, explaining that in the case of the general database intelligence system "very little time is dedicated to training members on how to use that system … you're just expected to use it." Training is a technical and organisational issue that may not be foreseen at the adoption stage. Where specialized software is used, technical training may be reduced but there will still be a need for officers to understand how to implement police responses in practice. This point was also made by two research participants from the same team from the United Kingdom component of the study, who had experience evaluating a predictive policing program:

> To me it's you get out of the car and you talk to people. It's really simple, but the implementation issues are still there. Cops don't get it. (ID removed)

> … [A]ctually all of [the software tested] were pretty accurate. But what my evaluation was … it was a process evaluation, and then if it had of been implemented properly, I would've looked at impact on crime. As it was, not many officers received information, there wasn't any clear guidance, clear information, [there] wasn't … an operational model as to why the officers needed this. It wasn't built in to the tasking process on the ground, so officers weren't getting it in the same way. … Why would you even expect to see reduction [in crime] when people aren't even using the maps they were given? (ID removed)

Comprehensible outputs

If the analysis is to be outsourced, it is most likely that one of the predictive software products mentioned above (or a similar product) would be licensed. This still requires financial resources, but relatively few additional human resources given the analytics is contained within the software itself. The outputs from predictive policing software tools are easily understandable by non-technical experts. Predpol®, for example, uses maps to show where crime is predicted as more likely to occur. Assuming the system itself is trusted (and the police do not wish to look into the black box), this reduces the human resource and training requirements. As one participant in a federal law enforcement agency noted, this can have significant resource implications:

> Because at the end of the day, I can have a great technical system that brings in all the data in the world and creates all these outputs but if at the end of the day if it doesn't work in with all the information that our investigators have in a way that they can understand, in a way they can draw the conclusions that they need, having all that data is of no use to them whatsoever. (ID removed)

Off the shelf predictive policing software can satisfy this need; police officers can understand what outputs mean (in particular, crime is more likely to happen in particular places) without opening the "black box" of the software itself. Further, the software resolves existing problems around information overload in managing and analyzing larger volumes of data, as the analysis is done within the software product itself. While this reduces *technical* training requirements, it does not reduce the need for training as to operational processes that will be adopted.

Complex, opaque products

Law enforcement agencies can find it difficult to select appropriate software products that meet their needs. One research participant, a law enforcement officer from a state police force (ID removed), was skeptical as to decisions made within law enforcement agencies about appropriate information technology: "traditionally and historically … has not been very good at IT infrastructure … we're police officers realistically, we're not IT experts". This does not necessarily mean that the initial purchasing decision will not be made, but if an inappropriate product is purchased, this may lead to challenges in technical implementation.

Algorithms used in predictive policing are typically complex and, where specialist software is purchased, are often non-transparent due to commercial confidentiality. This may not be attractive, particularly to front line police officers, who may feel that their understanding of the area and instinct is a better guide than computer software whose inner workings are opaque. Such skepticism about the ability of a computer to perform better than a human was discussed by one research participant who had worked in an intelligence organisation:

> The best analytical tools will always be in the human brain and identifying patterns that computers couldn't see then and can't continue to see now. So there are always limitations around what computers can and can't do. (ID removed - INTEL)

In addition, opacity raises issues for transparency and accountability of police decision-making, potentially generating legitimacy concerns in the broader community (see Bennett Moses and Chan 2014).

Infrastructure

In addition to a decision to purchase specific software, or hire analysts able to do it themselves, additional infrastructure would be required. The hardware required will vary, depending on the product being used – for a simple spreadsheet program, most computers would be sufficient, but other tools may require greater capacity. In some cases, outdated computers and storage facilities may need to be replaced with newer computers and more efficient data storage. While this increases the initial expense of adoption, it may enhance buy-in within the organisation.

Location-focus

Predictive policing software does not provide a complete tool for understanding crime. It focuses on one aspect of crime (location) and attempts to predict that. It does not explain *why* crime may happen or, with few exceptions (such as Chicago's heat lists), *who* will be the perpetrator or the victim. However, this does limit the effectiveness of predictive policing tools to those crimes where location likelihoods are predictable. This excludes crimes, such as kidnapping, where historic location has only a weak correlation with future location (Sherman et al. 1989: 47, Hart and Zandbergen 2012: 58). The relevance of such limitations will depend on the alignment between agency priorities and crime types that are predictable.

Data requirements

Predictive software tools require historic crime data, linked to particular locations, to make predictions. Two research participants expressed concern about data accuracy and verification (ID removed). Such issues are most likely to come to the forefront after the technology is deployed, depending on the extent to which leaders have insight into the limitations of data collection within their own agencies and, where relevant, beyond that. Predictive policing approaches rely on both accessibility of data currently held by law enforcement agencies and the accuracy or integrity of that data, which requires electronic recording of crime information, including relatively precise information about location. If accurate data is not used, this will negatively impact the technical implementation and effectiveness, the organisational culture (as inaccurate predictions lead to a loss of trust) and public legitimacy (if the public become concerned about wasted resources).

The precise data requirements of predictive policing software vary. As mentioned above, as well as crime data, particular approaches may rely on demographic data, rates of home foreclosures, weather patterns, geographic features and social media analysis. In some cases, there are practical challenges in procuring data, legal challenges restricting the availability of data or technical challenges in obtaining data in a useable format. In interviews, 11 participants from operational organisations mentioned legal requirements (real or perceived) as a barrier to data sharing, 9 mentioned technical issues and 6 mentioned cultural issues around data ownership and trust between data-holding agencies. The extent to which each of these types of issues arise depends on the data required for the predictive model being deployed. However, many predictive models are based on crime data that is likely to be held locally by a particular law enforcement agency, including the type and location of recent crimes. This works in favour of the technology's adoption and implementation.

Where predictive models require access to other data sets, this only works against adoption and implementation if police cannot use the need for predictive policing to justify access to more data. If Big Data analytics can lead to the removal of traditional legal restrictions on the use of data, it is likely to be embraced by police. It is, however, an open question as to how issues of intra-government data

sharing will be resolved. The value of privacy has been discussed extensively within academia, and is an issue that has attracted some citizen's groups. However, the complacency with which personal and private data is made available online by citizens has strengthened law enforcement agencies' case for disregarding privacy issues (or so they claim).

A question of organisational focus is whether the organisation is accustomed to analyzing trends, or tracking individuals. Pre-crime, disruption approaches can still be based on tracking and responding to the behaviour of individuals or networks of individuals rather than larger populations, as one research participant describes:

> One of the ideas around the National Disruption Group that we've set up is that everybody brings their data to the table *around a person of interest*. … In the disruption space we talk about … disruption plans where we bring that *assessment of an individual* together and put the options forward as to what the action might be. (ID removed, emphasis added).

Understanding and acting on broader trends rather than assessment of individuals requires a different focus from that which currently dominates within law enforcement. One interesting finding from our empirical study was the very limited extent to which data *currently* shared among law enforcement agencies is 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.
>
> It's no value if it's de-identified.
>
> It is possible that, in the future, police could use our data to predict trends....

Law enforcement agencies are more likely to communicate with each other about individual (or gang) threats than broader patterns and trends. While predictive policing can work on identified data, the lack of interest in de-identified data may signal a cultural wariness or unfamiliarity with trend analysis. This may ultimately affect the trust placed in predictive policing approaches.

Centralisation

Predictive policing would need to be administered centrally, at least within a police patrol jurisdiction. This runs counter to the desire of some police officers to have systems that support rather than replace their decision making, and available during patrols rather than from a central location. One research participant (ID removed) for example described the desire of some police "to have data on device when out on the streets when doing their job." (ID removed). Predictive policing works differently to systems such as CrimTrac which provide access to the underlying data "to enable more informed and empowered decision making" by the police officers themselves. (ID removed). The system runs centrally and front line police officers are sent to patrol particular locations. This is likely to be popular in police management as it provides managers with greater control over deployment decisions. However, there may be some police officers or line-level supervisors who do not fully implement a predictive policing program, continuing to patrol (at least in part) based on instinct rather than computer outputs. This may itself depend on how well predictive policing tools are explained and justified, for example through training programs. Some of the reactions of front-line police officers to being told where to patrol were observed by the two United Kingdom participants involved in the predictive policing evaluation:

> They don't necessarily like their roles pushed by evidence in that way. (ID removed)

> There was skepticism from officers, one of the maps that the police did looked like fishers. Just in terms of how they overlaid, and some officers found that funny. (ID removed)

However, implementation issues may be countered by the possibility of surveillance and monitoring of police to ensure that they patrol designated areas (Ericson and Haggerty 1997). Non-compliance with directions to patrol particular areas for particular lengths of time are easily noticed through geo-tagging police cars or tracking personal mobile devices. The ease with which compliance can be monitored and implementation measured likely works in favor of management interests, although it may lead to resentment among front line officers (Koper et al. 2014).

Discourse

Predictive policing discourse works in line with many aspects of police culture, particularly for police management. Predictive policing promises information in the otherwise unpredictable environment of crime. As one research participant stated "You can never be too well informed." (ID removed). Predictive policing builds on the broader mythology of Big Data to suggest that computers (with enough data) can be prescient and provide sufficient information for deployment decisions that themselves can "prevent" crime. Data analytics itself is "cutting edge", with strong scientific-technical credentials. Predictive policing thus frames a crime problem as something that can be solved *by police* (cf Dixon 2005), and particularly through "scientific" strategies of police management. The rhetoric of cutting edge, scientific, "smart" technologies for better policing outcomes is likely to be attractive.

Such positive beliefs around predictive policing are often based on a mythological and unrealistic view of actual capabilities and practices. As an example, one media article suggested that "[t]his complex equation can in theory predict, with pinpoint accuracy, where criminal offences are most likely to happen on any given day"(Adams 2012). It is clear that this statement is flawed, even "in theory", since the complexity of software goes beyond solving a single equation, no tool offers "pinpoint accuracy" but rather larger blocks (such as 500 square foot boxes or street sections) and not all "criminal offences" are equally suitable for forecasting. This may create issues at the implementation stage if the promises of the technology are not fulfilled.

The focus of predictive policing is crime prevention and disruption, rather than investigation of historic crimes. This is consistent with a temporal shift from post-crime to pre-crime approaches in policing (Zedner 2007) and shift in focus from punishment for moral failings to risk management and loss-prevention rather than punishment for moral failings (Zedner 2007, Ericson and Haggerty 1997). According to three research participants, this is a shift occurring at the moment in law enforcement in Australia from a prosecution-focus to a disruption-focus. While agency missions may be evolving, there was less agreement as to where they were along the path, as reflected in the views of three law enforcement managers from the same federal agency:

> …we'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, deterrents, target hardening and the likes. … [I]f 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. (ID removed)

> [W]e talk about a spectrum of activity. So we've got … traditional law enforcement so we always go for prosecution. If we can't prosecute we'll look for … an intervention like a control order or a preventative detention order and hey, we've had them for two years and we've

> only done two. But that indicates how the environment is changing. Then we'll go into the middle where we're looking at this sort of disruption thing. (ID removed)
>
> … we had pretty much moved away from the prosecution being the main focus. Disruption now is the main focus. (ID removed)

Predictive policing hinges on disruption being an important part of the organisational mission of a law enforcement agency. Given the spectrum of views, it is difficult to work out precisely how far law enforcement in Australia has moved from a prosecution-focused mission to a disruption-focused mission. However, given the movement seems to be in that direction, this points in favor of the adoption of predictive policing software at least over time.

Within the realm of pre-crime approaches, predictive policing is couched in the rhetoric of crime control rather than problem-solving policing. In particular, by focusing on "predicted" future crime locations, rather than on the history of particular places (as occurs with traditional hot-spot policing), problem-solving approaches are made more difficult. The obvious approach to preventing future crime at a location (rather than understanding historic crime at a location) is police deployment to deter crime or catch criminals in the act. Police at all levels of the organisation are likely to feel more at ease with this kind of rhetoric.

Not only does predictive policing offer the possibility of *informed* decision-making, it also creates an aura of neutrality. Because the patrol areas are determined "scientifically" rather than through human discretion, law enforcement agencies have a response to public accusations of bias as to where police patrol. The neutrality is illusory, for the reasons stated in Chan and Bennett Moses (unpublished), however the idea that decisions are made by a "neutral" machine can protect agencies against accusations of bias. The possibility of "neutral" decision-making in law enforcement may also be attractive to traditionally marginalized communities. For such communities, who have not been well-served by traditional "craft" based approaches to policing, and those with poor perceptions of police, the possibility of a neutral or scientific approach may be particularly appealing.

The discourse around predictive policing can also have negative, dystopian overtones. Popular culture has an important impact on how new technologies are perceived, not only within user institutions, but in the society more broadly (Tranter 2011). Predictive policing is often associated with the book/movie *Minority Report*.[4] That story involves PreCrime police who stop and arrest "murderers" before an offence is committed. The intelligence base is not data analytics but once-human Precogs who receive visions of the future. Further, predictive policing does not necessarily lead to arrests of those in the predicted crime locations (but see Ferguson 2012, explaining how predictive policing will have a significant effect on reasonable suspicion analysis in the United States). The potential negative impact of *Minority Report* on public perceptions of crime-control capabilities and misuse thereof was mentioned by one research participant in a federal law enforcement agency:

> So we've got … Enemy of the State, Minority Report … these popular imaginings of technical capacities and the misuse. (ID removed - LE)

This may have negative implications for how the community perceives predictive policing, even if the reality is a long way from dystopian fiction.

---

[4] Philip K Dick, 'Minority Report', Leo Margulies (ed), *Fantastic Universe* (January 1956); Minority Report (Dreamworks, Amblin Entertainment, 20th Century Fox, Cruise/Wagner Productions, Blue Tulip, 2002).

Finally, neighbourhoods (or individuals) identified for increased surveillance may be selected in ways that create tensions within the broader community (Bennett Moses and Chan, unpublished). Targeting may be ineffective, as where predictions are based on flawed data. Targeting may be unfairly selective or insufficiently precise. Finally, targeting (including in the above scenarios) may correlate with sensitive characteristics such as race or ethnicity. Where communities feel they are being unfairly targeted (or ignored) under a predictive policing program, this can affect the program's implementation and also, politically, its continued existence.

Technological momentum

The move to technology-driven solutions to policing problems has already begun. A great deal of police work is already being automated. Increasing use of telemetric policing (O-Malley 2013) is a good example of this. There may also be a belief that such changes are inevitable or required as part of maintaining security in today's world. This attitude was evident in some of the interviews:

> There is no escaping [digital and computer technology], "it is here". … Big Data is something that happens to us, not something we are asking for (ID removed - INTEL)

> From a security perspective, can we afford not to be constantly traversing data for patterns, anomalies? (ID removed - INTEL).

> As each new round of technology is rolled out we then look at it, utilise it, but then we start thinking about what additional features could be added or used to improve it. So it's a never-ending circle of improvement. (ID removed - INTEL)

This does not imply any technological determinism, but rather suggests a kind of technological momentum as the use of these kinds of technologies becomes an increasingly accepted aspect of police practice (see generally Hughes 1994).

5. Conclusions

As Koper et al. (2014:215) found in their research on the impact of technology on policing in the US that "the effects of technology in policing are complex and … advances in technology do not always produce obvious or straightforward improvements in communication, cooperation, productivity, job satisfaction, or officers' effectiveness in reducing crime and serving citizens". The effective implementation of technology can "depend on management practices, agency culture, and other contextual factors" (2014:215). In this paper, we look at a range of technical, practical and cultural features of predictive policing and how these were likely to impact on both the decision to use the technology and the impact and uptake of the technology in practice. We drew on interviews in Australian agencies, as well as our own research on predictive policing and the broader literature. Ultimately, like Willis and Mastrofski (2012:87), we find it hard to predict its impact. However, we have drawn out several strands that likely signal the factors likely to affect its successful implementation. Overall, most factors point in favour of its adoption, while successful implementation sits on the edge, with many potential avenues to failure or infidelity in implementation. The challenge here is without full compliance at the implementation stage, predictive policing tools are hard to evaluate – both as crime reduction devices and for broader social impacts. Although we are not convinced of the benefits of predictive policing approaches, adoption without successful implementation is likely the worst outcome. Thus, while not underestimating the importance of careful consideration of any decision to adopt predictive policing as an approach *at all*, we believe that any attempt to do so should not underestimate the importance of proper implementation and evaluation.

References

Adams, G., 2012. LAPD's sci-fi solution to real crime, *Independent*, 11 January, p. 32.

Australian Crime Commission, CEO Keynote address – International Serious and Organised Crime Conference (30 July 2013), published by ForeignAffairs.co.nz.

Beck, U. (1992). *Risk Society: Towards a New Modernity.* London: Sage.

Beck and McCue (2009) Predictive Policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession? *The Policing Chief* November 2009: 18-24.

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(2): 643

Bennett Moses, L. and Chan, J. (unpublished) Algorithmic Predictions in Policing: Assumptions, Evaluation and Accountability.

Bowers, K.J., Johnson, S.D. and Pease, K., 2004. Prospective hot-spotting: The future of crime mapping?. *British Journal of Criminology*, 44 (5), 641–658.

Braga, A.A., Papachristos, A.V. and Hureau, D.M. (2014) The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-Analysis. *Justice Quarterly* 31(4):633-663.

Braga, A. A., & Weisburd, D. L. (2007). *Police innovation and crime prevention: Lessons learned from police research over the past 20 years* (No. 218585). Washington, DC: National Institute of Justice.

Chan, J. (1997) *Changing Police Culture.* Melbourne: Cambridge University Press.

Chan, J. (2003) Police and new technologies in T. Newburn (ed) *Handbook of Policing*. Willan.

Chan, J. (2001) The technological game: How information technology is transforming police practice. *Criminology and Criminal Justice* 1(2):139-160.

Chan, J. & Bennett Moses, L. (2016) Is Big Data Challenging Criminology?. *Theoretical Criminology* 20(1):21-39.

Davenport, T.H. and Patil, D.J. (2012). Data Scientist: The Sexiest Job of the 21st Century. *Harvard Business Review* October 2012. https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/.

Darroch, S and Mazerolle, L (2012) Intelligence-Led Policing: A Comparative Analysis of Organizational Factors Inflencing Innovation Uptake. *Police Quarterly* 16(1): 3-37.

Dixon, D., 2005. Why don't the police stop crime? Australian & New Zealand journal of criminology, 38 (1), 4– 24.

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

Ericson, R.V. and Shearing, C.D. (1986) The Scientification of Police Work, in G. Böhme and N. Stehr (eds) *The Knowledge Society: The Growing Impact of Scientific Knowledge on Social Relations* Dordrecht: D. Reidel Publishing Company.

Ferguson, A.G. (2012). Predictive Policing and Reasonable Suspicion. *Emory Law Journal* 62:259.

Graziano, L.M., Rosenbaum, D.P. and Schuck, A.M. (2014) Building group capacity for problem solving and police–community partnerships through survey feedback and training: a randomized control trial within Chicago's community policing program. *Journal of Experimental Criminology* 10(1):79-103.

Hassell, D and Lovell, RD (2015) Fidelity of implementation: important considerations for policing scholars *Policing and Society* 25(5): 504-520.

Hughes, T. P. Technological momentum, in Smith, M.R. and Marx, L. eds., *Does Technology Drive History?: The Dilemma of Technological Determinism*. Massachusetts Institute of Technology. 101–113.

Hunt, P., Saunders, J., and Hollywood, J.S., 2014. *Evaluation of the Shreveport predictive policing experiment*. Santa Monica, CA: RAND.

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 Behavioural Aspects of Implementing Police Technologies. *Policing* 8(2):212-221.

Maguire, M., 2000. Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Policing and Society*, 9 (4), 315–336.

O'Malley, P (1992) Risk, power and crime prevention *Economy and Society* 21(3):252-275.

O'Malley, P. (2013). Telemetric Policing, in Bruinsma, G. and Weisburd, D (eds), *Encyclopedia of Criminology and Criminal Justice*. Springer. 5135..

Perry, W.L., McInnis, B., Price, C.C., Smith, S.C. and Hollywood, J.S., 2013. *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica, CA: RAND

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 (4): 711–729.

Sherman, L.W., Gartin, P.R., Buerger, M.E., 1989. Hot spots of predatory crime: Routine activities and the criminology of place. Criminology, 27 (1), 27–56.

Tranter, K. (2011) 'The Speculative Jurisdiction: The Science Fictionality of Law and Technology' *Griffith Law Review: Law Theory Society* 20(4):817-850.

van Brakel, R. and De Hert, P., 2011. Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies*. 20 (3), 163–192.

Weisburd, D. et al. (2010) Is problem-oriented policing effective in reducing crime and disorder? Findings from a Campbell systematic review. *Criminology & Public Policy* 9(1):139-172.

Weisburd, D., & Lum, C. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police Practice and Research: An International Journal*, 6(5): 419-434.

Willis, J.J. & Mastrofski, S.D. (2011) Innovations in Policing: Meanings, Structures and Processes. *Annual Review of Law and Social Sciences* 2011.7:309-334.

Willis, J.J. & Mastrofski, S.D. (2012) Compstat and the New Penology: A Paradigm Shift in Policing? *British Journal of Criminology* 52:73-92.

Zedner, L. (2007) Pre-crime and post criminology? *Theoretical Criminology* 11(2): 261-281.