USING BIG DATA FOR LEGAL AND LAW ENFORCEMENT DECISIONS: TESTING THE NEW TOOLS

LYRIA BENNETT MOSES[*] AND JANET CHAN[**]

I   INTRODUCTION

The term 'big data' has been described as a 'buzzword tsunami'.[1] It is easy to be excited about improvements in computing and, in particular, the ability to store and manipulate larger and more complex datasets for less money. There are many books devoted to articulating the extent to which these factors will have a significant economic impact, as well as guides on 'how to' use big data to grow or strengthen a business.[2] In the United States ('US'), the buzz associated with 'big data' in the business and IT communities has begun to colonise both legal practice and the administration of justice.[3] These analytical methods promise to provide ready answers to questions such as: what are the chances my client will succeed in litigation? What is the probability that a potential parolee will pose a danger to the community? Where are police resources most effectively employed? It has been suggested that, with sufficiently large datasets and the right analytics and machine learning techniques, we will have simple answers to traditionally difficult questions. Even though the analytics itself can only identify patterns in data, these patterns can be used to guide decisions. A low probability

1   Evgeny Morozov, *Your Social Networking Credit Score* (30 January 2013) Slate <http://www.slate.com/articles/technology/future_tense/2013/01/wonga_lenddo_lendup_big_data_and_social_networking_banking.html>.

2   See, eg, Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013); Jason Kolb and Jeremy Kolb, *The Big Data Revolution* (Applied Data Labs, 2013).

3   Big data can be defined in different ways (see Part II). In this article, we focus on big data analytics and, in particular, operations performed on large datasets in order to make generalisations and predictions that influence decision-making in legal and law enforcement contexts.

of success in litigation can lead to a different approach to settlement negotiations. Quantitative analysis that calculates the risk a prisoner will pose to the community can govern parole decisions. Empirically derived 'hotspots' or 'hot lists' of potential criminals can change policing strategies. In each of these cases, quantitative information about correlations and probabilities can be converted into real-world actions through its influence over human decisions.

Predictive techniques based on big data are already being used in both private and public decision-making and, in particular, by legal practitioners, judges and police. On the private side, software is being developed to predict the outcomes of legal disputes. Lex Machina is a private analytics company founded in 2010 aiming to predict the cost and outcome of intellectual property litigation.[4] A predictive model has been developed tracking settlement outcomes of securities fraud class action lawsuits.[5] Big data can also be used in electronic discovery to decrease the costs of civil litigation.[6] In the public sector, data analytics has been used in some US jurisdictions to make decisions about bail based on 'an objective, scientific measure of risk'.[7] A recent Arnold Foundation report advocated growth of less than 10 per cent of US jurisdictions using data analytic tools in pre-trial decision-making, arguing this tool should be available to all judges as an aid to pre-trial decision-making in order to 'make our communities safer and stronger, our corrections budgets smaller, and our system fairer.'[8] Big data analytics may also be relevant in post-conviction decisions. Some jurisdictions, such as Virginia, link parole decisions to statistical data concerning rates of reoffending for people in different categories.[9] It is based on a points system, which counts how many factors, statistically aligned with reoffending rates, are present in a particular case. Some of these are intuitive and likely to be relevant even in the absence of data, such as the number of past convictions. Others, such as the gender of the victim in sex offences, are both less intuitive and more problematic. Predictive policing is also being explored in some jurisdictions as a means of optimising police deployments to match predictions

---

4   Lex Machina, *About Us* (2014) <https://lexmachina.com/about/>.
5   Blakeley B McShane et al, 'Predicting Securities Fraud Settlements and Amounts: A Hierarchical Bayesian Model of Federal Securities Class Action Lawsuits' (2012) 9 *Journal of Empirical Legal Studies* 482.
6   See, eg, Nicholas M Pace and Laura Zakaras, 'Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery' (Monograph, RAND Institute for Civil Justice, 2012) 62–6. <http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf>; Tonia Hap Murphy, 'Mandating Use of Predictive Coding in Electronic Discovery: An Ill-Advised Judicial Intrusion' (2013) 50 *American Business Law Journal* 609.
7   See Anne Milgram, *Why Smart Statistics Are the Key to Fighting Crime* (October 2013) TED 8:48 <http://www.ted.com/talks/anne_milgram_why_smart_statistics_are_the_key_to_fighting_crime/transcript#t-27602>.
8   Laura and John Arnold Foundation, 'Developing a National Model for Pre-trial Risk Assessment' (November 2013) 5 <http://arnoldfoundation.org/sites/default/files/pdf/LJAF-research-summary_PSA-Court_4_1.pdf>.
9   Bernard E Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (University of Chicago Press, 2007) 13–14.

about *who* will commit crimes and *where*.[10] These uses are currently relatively small-scale, and mainly confined to the US, although Australia is beginning to recognise the potential of big data analytics, with growing interest and investment in research in that field. For example, the government recently invested $25 million to set up a Cooperative Research Centre (Data to Decisions CRC) to 'develop robust tools to maximise the benefits that Australia's defence and national security sector can extract from big data to reduce national security threats.'[11]

   This article aims to describe the potential applications of big data tools for legal and police decision-making, compare these to historical precedents in order to better understand what is new about these tools, and evaluate them by reference to technical, social and normative criteria. While the early stage of diffusion of this technology, and hence its amorphous form, makes such an evaluation challenging, this fluidity also provides an opportunity for designers and potential users to reflect on, and take account of, the issues we raise in the development, implementation and operation of these tools. Thus we hope that the concerns we raise will heighten awareness among developers and potential users prior to the 'hardening' of the socio-technical structures supporting big data.[12]

   We begin in Part II by introducing big data analytics and summarising its techniques and capabilities. In particular, we describe what kind of information they provide, how they work, what kinds of inferences can be drawn and how they can lead to real-world action. We explain how big data is an extension of earlier statistical techniques, and an example of a turn to empirical approaches to decision-making.

   In Part III, we introduce a three-dimensional framework to evaluate the use of big data technologies in legal and policing decision-making. We argue that, at an early stage of a technology's development, there are three lenses through which its potential and impacts can be evaluated. The first of these is to consider the technical functionality of a technology, taking account of its purpose, effectiveness and efficiency. Secondly, one can look at the likely take-up of the technology, examining the extent to which the 'technological frame' of the designers aligns with that of the potential users. Finally, one can adopt a normative stance and consider the benefits and harms of potential applications of the technology. While there are overlaps between these categories (so that diffusion of a technology is linked to its effectiveness and perceived value), they are useful for drawing out the relevant elements for evaluating the use of big data in particular contexts.

---

10   Craig D Uchida, 'Predictive Policing' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer, 2013) 3871, 3871.

11   See Ian Macfarlane, 'Driving Research and Delivering Results for Australia' (Media Release, 21 February 2014) <http://minister.innovation.gov.au/ministers/macfarlane/media-releases/driving-research-and-delivering-results-australia>. The authors will be key researchers in this Centre; however, the opinions expressed in this article do not represent those of the Centre.

12   Langdon Winner, 'Do Artifacts Have Politics?' (1980) 109(1) *Daedalus* 121, 127–8.

In Part IV, we consider the socio-technical landscape for legal and law enforcement decision-making before the potential deployment of big data analytic tools. This serves two purposes. First, it provides a suitable testing bed for the evaluative framework described in Part III. One can see how legal and law enforcement values and cultures have impacted on the practices that developed around earlier decision-making tools. Second, it provides a useful background against which big data tools can be understood. We explain that while legal expert systems sought to mirror the thought processes involved in doctrinal legal reasoning, both police information systems and sentencing databases were originally driven by a data-oriented vision but adapted to work within more traditional technological frames. Understanding the continuities and differences between big data and precursor technologies will prove important for evaluating the likely uptake and impact of new analytic tools.

In Part V, we evaluate big data tools by reference to the criteria developed in Part III. Our focus here is on the analytics itself and the use of quantitative data by judges, lawyers and police for drawing inferences and making decisions in both public and private contexts.

We summarise our analysis and conclusions in Part VI. We will argue that the evaluation of big data analytic techniques ought to go beyond questions of accuracy and reliability, to concerns about their impact on justice outcomes, the importance of transparency and accountability in public decision-making and the appropriateness of relying upon algorithmically derived extra-legal factors. Big data techniques face similar limitations to earlier empirical techniques, but their enhanced power and reduced transparency combine to increase the potential for inappropriate uses. We should be wary of overly optimistic predictions as to the transformative power of big data analytics in enhancing legal and law enforcement decision-making, particularly where the techniques operate within a black box.

There are thus two issues we do not address in this article. The first is privacy issues relating to the collection and storage of the data that is analysed. While such issues are not unimportant, they have been the focus of considerable attention from legal scholars, technologists and the media,[13] particularly when

---

13   For legal writing, see, eg, Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 239; Woodrow Hartzog and Evan Selinger, 'Big Data in Small Hands' (2013) 66 *Stanford Law Review Online* 81 <http://www.stanfordlawreview.org/online/privacy-and-big-data/big-data-small-hands>; Felix T Wu, 'Defining Privacy and Utility in Data Sets' (2013) 84 *University of Colorado Law Review* 1117; Dennis D Hirsch, 'The Glass House Effect: Big Data, the New Oil, and the Power of Analogy' (2014) 66 *Maine Law Review* 374; Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 *International Data Privacy Law* 74; Julie E Cohen, 'What Privacy Is For' (2013) 126 *Harvard Law Review* 1904. For interest from technologists, see, eg, Ann Cavoukian and Jeff Jonas, *Privacy by Design in the Age of Big Data* (8 June 2012) Policy by Design <http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf>; Julie Brill, 'A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data' (Speech delivered at the Sloan Cyber Security Lecture, The Polytechnic Institute of New York University, 23 October 2013). Media interest grew substantially after the Snowden revelations.

compared to issues associated with the analytic techniques themselves. Further, the US President's Council of Advisors on Science and Technology recently recommended an approach that focuses on the *use* rather than the *collection and storage* of data, because of feasibility concerns and the fact that it is primarily use that is associated with harm.[14] The second issue we largely avoid concerns the generation of legal outcomes in the absence of human decision-making, as occurs when a fine is automatically issued by a machine upon receiving input from a sensor. While this kind of 'telemetric policing' raises questions beyond those discussed here (being an extreme of non-transparency and non-accountability),[15] we believe the evaluation framework developed here provides a useful starting point.

II   WHAT IS BIG DATA?

The techniques that comprise big data analytics are significantly older than the current hype associated with big data technology. While enhancements in computing power have enabled the constructive use of large datasets, big data analytics has its origins in an 'empirical turn' in computing tools for legal decision-making, that is the use of statistics and machine learning.

A   Empirical Approaches and Techniques

> The prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law.[16]

Traditionally, legal and justice decisions are generally made on the basis of intuition, professional expertise and experience. An empirical approach to legal decision-making seeks to base such decisions on statistical evidence. Loevinger, one of the early proponents of jurimetrics, was inspired by Holmes's point of view, as captured in the quotation above.[17] He was a rule-sceptic, lacking faith in automated manipulation of legal rules through expert systems on the basis that 'we have no terms to put into the machines … Legal terms are almost all vague verbalizations which have only a ritualistic significance.'[18] In his view, knowledge about law could best be acquired through observation using scientific methods, in particular through the empirical study of legal phenomena with the aid of mathematical or statistical models.[19] Information would be gleaned, not

---

14   President's Council of Advisors on Science and Technology, 'Report to the President – Big Data and Privacy: A Technological Perspective' (Report, May 2014).

15   See generally Pat O'Malley, 'Telemetric Policing' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer, 2013) 5135.

16   O W Holmes, 'The Path of the Law' (1897) 10 *Harvard Law Review* 457, 461.

17   Lee Loevinger, 'Jurimetrics: The Next Step Forward' (1949) 33 *Minnesota Law Review* 455.

18   Ibid 471.

19   Ibid 471 ff; Richard De Mulder, Kees van Noortwijk and Lia Combrink-Kuiters, 'Jurimetrics Please!' (2010) 1(1) *European Journal of Law and Technology* <http://ejlt.org//article/view/13/12>.

from mirroring the thought process of judges, but by observing their behaviour. For example, using statistical techniques, it is possible to test for correlation between particular characteristics of judges and their tendency to decide in favour of a particular side in a dispute.[20]

Like older statistical techniques, machine learning is based on drawing inferences from observations, but the move to machine learning turns conventional statistical inference on its head. Traditionally statistical inference is driven by hypotheses derived from theories or past research. Instead of testing hypotheses, machine learning analyses 'training' data and, through the use of an algorithm, identifies the 'best' hypothesis linking input data to outputs. The 'training' data is simply the examples (perhaps extracted from historical records) fed into the algorithm, from which it 'learns' potential predictive relationships. Despite being driven by algorithms, machine learning does not take place without human involvement, input and assumptions. In particular, the design of the learning exercise will necessarily introduce some inductive bias whenever the computer learner is asked to classify unseen examples. Inductive bias refers to the assumptions that are used to predict outputs given inputs outside the training set; for example, an algorithm may be biased towards simpler hypotheses or make assumptions about which elements are treated as potentially relevant in formulating a hypothesis.[21] It is humans who set up the machine learning algorithm, and who make decisions about what type of machine learning to use, which datasets to employ in the analysis, how much data to include in the training set, in what ways the data is 'cleaned', what kinds of hypotheses to consider and what validation is appropriate.

Machine learning takes different forms, but some basic examples provide a useful insight into this approach to drawing inferences. A machine might be asked to identify the simplest *decision tree* that explains data in the training set, in which case the inductive bias is a preference for simpler trees over larger, more complex, trees. In form, the result (a decision tree) looks a lot like a legal rule, and can be written as a sequence of *if … then …* statements. *Neural networks* are another example of machine learning. A neural network has an initial structure chosen by a human, who decides how many layers of 'neurons' to use between the input and the output. These neurons are connected, so that a particular neuron fires only where it receives particular inputs from other neurons. The network can learn from a training set of past examples, adjusting the circumstances in which neurons fire depending on the network's performance over the training set. While significantly more complex than simple decision trees, neural networks can be made to generate statements that explain how the inputs contributed to the output,[22] although not necessarily in a form that makes it

---

20 Stuart S Nagel, 'Judicial Backgrounds and Criminal Cases' (1962) 53 *Journal of Criminal Law, Criminology and Police Science* 333.

21 Tom M Mitchell, *Machine Learning* (McGraw-Hill, 1997) 39–45.

22 David R Warner Jr, 'A Neural Network-Based Law Machine: The Problem of Legitimacy' (1993) 2 *Information & Communications Technology Law* 135, 141.

easy for a human to understand the relationship. A neural network can be used for drawing legal inferences, for example by 'learning' to estimate the quantum of damages for whiplash injury from past legal outcomes without being told the legal rule used to derive those outcomes.[23] Particularly useful in predicting legal outcomes is *Bayesian learning*. This provides a flexible approach to learning – observed training examples increase or decrease the probability that any particular hypothesis is correct, meaning that a hypothesis that is inconsistent with part of the training set is not excluded, just demoted. Bayesian prediction is not limited to particular correlative factors, but takes account of the fact that some factors will have increased influence if other factors are also present. Further, Bayesian learning can factor in prior knowledge, such as that inherent in legal rules, by assigning a 'starting' probability to different hypotheses. Bayesian learning allows one to estimate the probability of a particular outcome (such as the result of a case) by reference to a calculation 'derived' from data in the training set. In the policing context, *random forests* have been considered the most effective tool. In this approach, the algorithm grows multiple decision trees (and does not rely on only the simplest tree), and then counts the number of trees that predict a particular outcome (such as a crime occurring in a particular location).[24]

Despite the rule-scepticism motivating the early legal empiricists, machine learning is still rule-based. The 'rules' identified through machine learning may look more complex than rules familiar to law students, and they will contain different elements whose relevance may not be immediately obvious. Neural networks, for instance, generate highly complex rules which are generally 'hidden', but nevertheless present.[25] Because machine learning relies on rules, it is only possible to draw useful inferences in circumstances where there is a degree of regularity that can be modelled. The rule-scepticism that favours empirical approaches is thus not scepticism about the ability of rules to form a basis for making predictions about legal outcomes, but the *type* of rules that are most useful for doing so. Whereas traditional doctrinal reasoning assumes the usefulness of legal rules for drawing inferences about legal outcomes, empirical approaches typically treat legal explanations as (potentially) of equal importance as non-legal explanations. Of course, it is *possible* that the rule generated by a machine learning algorithm will correspond, either absolutely or in part, with a recognised legal rule.[26] Indeed, a learning activity could be set up employing a

---

23   Andrew Terrett, 'Neural Networks: Towards Predictive Law Machines' (1995) 3 *International Journal of Law and Information Technology* 94.

24   Uchida, above n 10, 3876. Richard Berk, 'Forecasting Methods in Crime and Justice' (2008) 4 *Annual Review of Law and Social Science* 219; Richard Berk, 'Asymmetric Loss Functions for Forecasting in Criminal Justice Settings' (2011) 27 *Journal of Quantitative Criminology* 107.

25   Warner, above n 22.

26   See, eg, Laurent Bochereau, Danièle Bourcier and Paul Bourgine, 'Extracting Legal Knowledge by Means of Multilayer Neural Network Application to Municipal Jurisprudence' in Marek Sergot et al (eds), *Proceedings of the Third International Conference on Artificial Intelligence and Law* (ACM Press, 1991) 288.

training set comprising hypothetical applications of an already known legal rule (although that would seem a futile exercise).[27] The point here is merely that the rules identified through machine learning or statistics need not be limited to legally relevant inputs.

B Defining Big Data

Different definitions of big data have been offered. A common definition, which describes problems to be overcome in dealing with big data, is to refer to the 'three Vs'. These are the increased Volume of data, the increased Velocity with which it is produced and processed, and the increased Variety of data types and sources.[28] Each of these Vs poses a technical challenge to the traditional way that data has been stored, processed and analysed, typically through the use of relational databases. Big data is a term that covers the many new tools that can quickly process larger volumes of data coming from diverse sources with different data structures. A similar definition has been offered by the McKinsey Global Institute, which defines big data as 'datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze',[29] a definition that deliberately moves with technological advances over time. The size and complexity of datasets being analysed is important for several reasons. As the size of datasets increases, one can gain insights from analysis despite the fact that some of the data contains errors.[30] Big data also allows analysts to shift from analysing sample data in order to make inferences about a population, to analysing data pertaining to the entire population, sometimes described as 'N = all'.[31]

This approach to data analysis has been useful in a wide variety of contexts. For example, it can be used to monitor disease outbreaks,[32] evaluate credit risk,[33] predict insurance outcomes,[34] enable emergency response,[35] improve

---

27 Dan Hunter, 'Out of Their Minds: Legal Theory in Neural Networks' (1999) 7 *Artificial Intelligence and Law* 129, 135, 137, 144.

28 Gartner, 'Gartner Says Solving "Big Data" Challenge Involves More Than Just Managing Volumes of Data' (Press Release, 27 June 2011) <http://www.gartner.com/newsroom/id/1731916>.

29 James Manyika et al, 'Big Data: The Next Frontier for Innovation, Competition and Productivity' (McKinsey Global Institute, May 2011) 1 <http://www.mckinsey.com/~/media/McKinsey/dotcom/ Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data _full_report.ashx>.

30 Mayer-Schönberger and Cukier, above n 2, 13.

31 Mayer-Schönberger and Cukier, above n 2, 26.

32 Jeremy Ginsberg et al, 'Detecting Influenza Epidemics Using Search Engine Query Data' (2009) 457 *Nature* 1012; but see Declan Butler, 'When Google Got Flu Wrong' (2013) 494 *Nature* 155.

33 Morozov, above n 1.

34 Charles Nyce, Australian Institute for CPCU/Insurance Institute of America, *Predictive Analytics White Paper* (2007) <http://www.theinstitutes.org/doc/predictivemodelingwhitepaper.pdf>.

35 Mark Anderson, *Emergency Alert Study Reveals Metadata's Better Side* (24 July 2013) IEEE Spectrum <http://spectrum.ieee.org/computing/networks/emergency-alert-study-reveals-metadatas-better-side/ ?utm_source=techalert&utm_medium=email&utm_campaign=072513>.

retail and manufacturing,[36] and conduct text analysis.[37] Further, as computers are increasingly able to work with more complex inputs (documents rather than databases), big data can be released onto legal texts (including pleadings, judgments, affidavits and settlement agreements) to identify potentially unknown correlations between verbal formulas and legal outcomes. This would in theory allow for the calculation of probabilities of success in court, and an estimation of damages likely to be awarded in court or through negotiation given a list of statements about facts and context of a dispute. We are not there yet, but that is the direction in which these technologies are moving.

A very different definition of big data has been proposed by boyd and Crawford:

> We define Big Data as a cultural, technological, and scholarly phenomenon that rests on the interplay of:
>
> (1) *Technology*: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets.
>
> (2) *Analysis*: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims.
>
> (3) *Mythology*: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy.[38]

The first two elements of this definition highlight two of the different stages of employing big data tools. There is the actual technical element (the ability to store and manipulate large datasets) as well as the 'data analysis'. In our view, the analysis itself can be divided into stages – the identification of correlations and relationships (generally relying on statistical inference or machine learning) and the use of these to make broader claims within fields such as law. The first step involves calculation, the second drawing inferences, not just about the data and what it reveals, but also about other things. Data may reveal that particular characteristics are associated with high reoffending rates; an inference may then be drawn as to a desirable legal result – that people with those characteristics not be granted parole.

The element of mythology depends on attitudes to the technology over time, both among particular professional groups that might use it, and in society more broadly. The temptation to mythologise the numbers generated by big data may be the result of increasing scepticism about models and expertise.[39] In the legal realm, this equates to scepticism about traditional doctrinal legal reasoning as a basis for predicting what a court will decide. If lawyers are sceptical about their

---

36   Manyika et al, above n 29.

37   Stephen Ramsay, *Reading Machines: Towards an Algorithmic Criticism* (University of Illinois Press, 2011).

38   danah boyd and Kate Crawford, 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2012) 15 *Information, Communication & Society* 662, 663 (emphasis in original) (citations omitted).

39   Mark Andrejevic, *Infoglut: How Too Much Information Is Changing the Way We Think and Know* (Routledge, 2013).

ability to predict the outcome of a legal dispute by 'thinking like a lawyer' (finding legal rules and precedents, applying them to the facts of a case, generating conclusions), then a number that seems to capture the answer they need to make decisions about commencing proceedings or settling disputes seems very tempting. This is especially so if they have a deeper understanding of the limits of traditional doctrinal techniques for making predictions than they have of the techniques used to generate the number. In particular, while lawyers are often sceptical about the ability of 'rules' to predict outcomes, it is rarely observed that machine learning also employs rules to make predictions, albeit rules that were generated by a learning algorithm rather than a traditional source of legal authority. However, it is not yet clear whether these technologies will be embraced by legal and law enforcement professionals or whether they will come to be seen as mythologically accurate. The buzz in the business and information technology worlds may not translate into these more traditional professional communities.

In our view, boyd and Crawford also omit a final stage relevant to big data: action taken on the basis of inferences drawn. This might be a decision to make a settlement offer, a decision to structure a transaction in a particular way, a decision to grant or withhold bail or parole or a decision to focus policing resources on particular locations or people. Potentially, such actions could be tied to mythology, in that action is taken based on beliefs about the 'higher form of intelligence' that big data represents, but this link is contingent. Action could be based on careful curation of datasets, limited and appropriate inferences and rational approaches to action. While mythology is contingent, the performing of algorithms and calculations, the drawing of inferences and the taking of action are all important stages in the use of big data analytics in legal and law enforcement decision-making.

III   A FRAMEWORK FOR TESTING BIG DATA

Although it may be too early to assess the impact of big data analytics on legal and policing practices, we can draw on the literature on technological change to construct a framework to help us test the potential, likely impact, and suitability of the new tools. It is important, first of all, to recognise

> that technology should not be seen as consisting of a physical, material dimension only; rather, technology operates in a social context and its meaning is perceived differently by people in different social and organisational positions. While technological changes have the capacity to transform social and organisational life, technology is itself shaped by social and organisational conditions.[40]

---

40   Janet B L Chan, 'Police and New Technologies' in Tim Newburn (ed), *Handbook of Policing* (Willan Publishing, 2003) 655, 668–9 (citations omitted).

Thus big data analytics in legal and law enforcement decision-making can be assessed along three dimensions: technical, social, and normative. The technical dimension considers practical issues of functionality and effectiveness, while the social dimension analyses the socio-cultural-political factors that may impact on uptake and penetration, and the normative dimension investigates the extent to which the new technology fits with the ethics or values of users and the general community.

A   Technical Dimension – Functionality and Effectiveness

Questions about functionality and effectiveness are fundamental to the evaluation of a technology. If technology does not work or does not help do things better or more efficiently, it is unlikely to be taken seriously. Of course, sometimes a faulty technology gains acceptance despite flaws, either because alternatives are not available or because the flaws are unknown, but a technology that fails the basic functionality test will be unlikely to prevail over the longer term. If early adopters have demonstrated failure in using particular tools, few others will come to emulate them.[41] Technical effectiveness is not only about the design and performance of the technology. It is often related to its management and implementation, for example, the adequacy of infrastructure, degree of integration with existing tools, and availability of high-quality training and support.[42]

B   Social Dimension – Uptake and Impact

The uptake and impact of technology by practitioners can vary depending on the type of technology and their perceived costs and benefits for potential users. In addition to relative advantage over earlier technologies, compatibility with the potential user's values, relative complexity, trialability (whether it can be tested) and observability (the extent to which the innovation is visible to others, creating network effects) are important factors affecting the adoption of technology.[43] Technological change has the potential to destabilise existing power structure and challenge accepted assumptions, work practices and values.[44] Thus the uptake and impact of new technology can be enhanced or limited by the extent to which there is congruence between the 'technological frames' of the technology designers and those of the users. Technological frames are cultural assumptions held by social groups regarding the capability, purpose, intended usage and likely

---

41   Patrice Flichy, *Understanding Technological Innovation: A Socio-Technical Approach* (Edward Elgar, 2007) 11.

42   Chan, above n 40, 671.

43   Everett M Rogers, *Diffusion of Innovations* (Free Press, 5th ed, 2003) 36, 219–66.

44   Peter K Manning, 'Information Technology in the Police Context: The "Sailor" Phone' (1996) 7(1) *Information Systems Research* 52, 54; Wanda J Orlikowski and Daniel Robey, 'Information Technology and the Structuring of Organisations' (1991) 2 *Information Systems Research* 143, 155; Richard V Ericson and Kevin D Haggerty, *Policing the Risk Society* (Oxford University Press, 1997) 411–12; Chan, above n 40, 664–5.

consequences of a particular technology.[45] Where technology is designed with the intention of changing existing culture of practice, users may avoid this change or exploit it for their own purposes.[46]

Of course, the binary options of 'adopt' or 'reject' are too simplistic, since technology may be adopted but not on the basis of the developer's technological frame. Rather than focusing on technology adoption, it is more helpful to ask how a technology might be used for what kinds of purposes and how that might influence decision-making.[47] Adoption itself may also take a variety of forms and involve a dynamic process. For example, big data analytics may be accepted at an organisational level but avoided at the individual decision-making level. Alternatively, it may be resisted initially but received favourably as users become more familiar with its capability. Finally, it may be adopted but used for different purposes from what was intended. Since cultural values and practices can change, for example in response to global trends, predicting what technologies will be used in the future, and what form they will take, is inherently difficult.[48] Nevertheless, compatibility with culture and values is an important consideration in predicting the adoption of particular technological practices. This leads us to the third set of considerations.

C   Normative Dimension – Ethics and Values

Whether a technology fits with the ethics and values of the users and the general community is an important criterion for evaluation. While the community may derive benefits from the adoption of a particular technology, they may not wish to sacrifice certain deeply held values for the sake of technological progress. Similarly, regardless of the sophistication of a new technology, legal and justice practitioners may be reluctant to rely on it if they feel that their professionalism is compromised in the process. Among the values held deeply by both professionals and community are those related to the fundamental premises of the rule of law in a democracy: legality, accountability and transparency.

It is important that decisions by judges and police *comply with legal rules*, such as may be found in international treaties, legislation or common law. The norms of relevance here are that decisions be based on legally relevant factors where that is required, that decisions do not discriminate on non-permissible

---

45   Wanda J Orlikowski and Debra C Gash, 'Technological Frames: Making Sense of Information Technology in Organisations' (1994) 12 *ACM Transactions on Information Systems* 174, 178.

46   See Chan, above n 40, 672–3.

47   Trevor J Pinch and Wiebe E Bijker, 'The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other' in Wiebe E Bijker, Thomas P Hughes and Trevor Pinch (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (MIT Press, 1987) 17; Flichy, above n 41, 90–1.

48   David E Nye, 'Technological Prediction: A Promethean Problem' in Marita Sturken, Douglas Thomas and Sandra Ball-Rokeach (eds), *Technological Visions: The Hopes and Fears That Shape New Technologies* (Temple University Press, 2004) 159 (on the challenges of prediction); Chan, above n 40, 669–70 (on influence of global trends).

grounds such as race,[49] and that people are treated as innocent until proven guilty.[50] Clearly, these are crude statements of complex and often subtle concepts. A high level of generality is sufficient, however, for preliminary exploration of technological practices that are not yet fully developed or implemented.

Similarly, it is often important that decision-makers are *accountable* for their decisions. The importance of accountability for judicial decisions is reflected in the requirement for judges to give reasons for their decisions, which are published in the judge's name. Accountability is also important in legal practice, in particular in the relationship between practitioner and client.[51] Police accountability is similarly demanded by the community and, in principle at least, embraced by police forces, as seen in their codes of conduct and statements of values.[52] The presence or absence of accountability is not the only consideration – one needs to know who is accountable to whom and for what.[53] This will depend on the context, and will vary both within and between different organisations and professional groups. For example, in the context of policing, accountability has two meanings: the control over police and the requirement to give accounts or explanations about conduct.[54] In evaluating a tool used to assist in making decisions, it is important to consider its potential effects on the different ways in which the decision-maker is accountable for his or her decisions.

Related to the requirements of accuracy, accountability and legality, is the need for *transparency*. Transparency enables detection of inaccuracy or faulty logics. It may be required to facilitate natural justice to those affected by decisions.[55] Transparency is particularly important whenever accountability is lacking. While human decision-makers may not be entirely transparent in their internal reasoning processes, at least they can be held personally accountable.

---

49   This is a requirement of Commonwealth and state legislation as well as the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 2(1) ('*International Covenant on Civil and Political Rights*').

50   This is a requirement of the *International Covenant on Civil and Political Rights* art 14(2).

51   The importance of this value is reflected in the title of Ysaiah Ross and Peter MacFarlane, *Lawyers' Responsibility and Accountability: Cases, Problems and Commentary* (LexisNexis Butterworths, 4th ed, 2012).

52   See NSW Police Force, *Standards of Professional Conduct* (2008) 3 <https://www.police.nsw.gov.au/__data/assets/pdf_file/0009/87993/SPC_Conduct_2008_INTRANET_230608.pdf> (listing accountability); Victoria Police, *Victoria Police Manual – Policy Rules: Professional and Ethical Standards*, 2 <http://www.police.vic.gov.au/retrievemedia.asp?Media_ID=53208> (referring to the importance of taking responsibility). But see David Dixon, 'The Normative Structure of Policing' in David Dixon (ed), *A Culture of Corruption: Changing an Australian Police Service* (Hawkins Press, 1999) 69 for the disjuncture between official principles, found in documents like statements of values and codes of ethics, and actual practice.

53   Martin Lodge, 'Accountability and Transparency in Regulation: Critiques, Doctrines and Instruments' in Jacint Jordana and David Levi-Faur (eds), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar, 2004) 124.

54   See Janet B L Chan, 'Governing Police Practice: Limits of the New Accountability' (1999) 50 *British Journal of Sociology* 251, 252.

55   Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249.

The ability to link decisions to a non-transparent tool, designed by others, or to 'facts' derived from an external non-transparent process, can diminish such personal accountability. Finally, transparency is essential for ensuring legality, providing a check on illegitimate state actions.

* * *

In summary, the above discussion shows that the potential, likely impact and suitability of big data technology for legal and justice decisions can be assessed along three dimensions: technical, social and normative. These considerations can be reduced to three primary criteria for evaluation: (1) whether big data technology can be successfully implemented to achieve better outcomes for legal and justice decisions; (2) whether particular applications will fit within the technological frames of potential users among legal and justice practitioners; and (3) whether it can be used in a way that conforms to the values of the professional and larger communities. We will label the first criterion 'effectiveness', the second 'acceptability' and the third 'appropriateness'.

IV   LESSONS FROM OLDER DECISION TOOLS

Big data analytics is the most recent evolution of a long line of computer-based tools offered for guiding legal and law enforcement decisions. In order to understand how big data analytics compares with existing practices and technological frames, it is necessary to reflect on key lessons in the history of decision-support tools for judges, legal practitioners and police. In this section, we briefly describe some of the earlier tools, focusing on their acceptance by professional communities and their impact on practice. As will become clear, instead of the tool reshaping practice, in every case the tool was adapted to better conform to the pre-existing technological frames of the users, viewed either as individuals or organisations.

A   Legal Expert Systems: A Decision-Support Tool Explicitly Based on 'Traditional' Reasoning

Unsurprisingly, early decision-support tools for judges and lawyers attempted to mirror traditional reasoning processes. In this respect, the designers of these tools and the community of users had similar technological frames. In the 1970s and 1980s, discussion of the use of computers in legal decision-making focussed primarily on the design of 'expert systems'. Expert systems are 'computer programs which perform complex tasks at a level which is at or near the level expected of a human expert.'[56] Legal expert systems thus have the goal of mimicking legal expertise – using a computer program to model how a lawyer might go about answering particular legal questions. It was felt that '[a] legal

---

56   Alan Tyree, *Expert Systems in Law* (Prentice Hall, 1989) 1.

expert system must not only arrive at the correct decision, but must arrive at it in the correct way.'[57] The computer program does not derive the expertise itself – the structure of a legal domain and raw legal information were all 'fed' into the system, sometimes separately to the main program itself,[58] which contained the inference engine.

The goal of expert systems, as the name implies, was to model how a legal expert would resolve a particular question. Thus a good expert system could give 'reasons' for conclusions reached, either in the form of a series of logical statements or through citations to relevant sources of law. Its output was thus not only the legal conclusion itself, but also a statement as to *why* that conclusion was reached. An ideal expert system would approach 'isomorphism', in that it would mirror the legal domain being modelled.[59] This required transparency, both to give 'reasons' and to enable updates.[60]

Despite the enthusiasm of computer scientists, lawyers and certainly legal theorists were aware of the limitations of such systems.[61] The main critique related to the *effectiveness* of these systems, being their ability to accurately mirror the reasoning of a legal expert. Not only are legal rules often contradictory, circular, ambiguous or deliberately vague or contestable, but they rely on social context and human interpretation and cannot be applied directly to raw facts.[62] A computer relying on logic may be able to manipulate legal rules, but interpretation and identification of exceptions will often require a human to identify a rule's purpose based on an understanding of its context.[63] Legal expert systems could thus not 'solve' difficult legal problems. Devices to deal with these limitations, including alternative pathways reflecting opposing interpretative views,[64] and fuzzy logic allowing for fractional truth values,[65] were insufficient to manage these problems.

---

57   T J M Bench-Capon, 'Deep Models, Normative Reasoning and Legal Expert Systems' in Edwina Rissland et al (eds), *Proceedings of the Second International Conference on Artificial Intelligence and Law* (ACM Press, 1989) 37.

58   See, eg, Tyree, above n 56, 9.

59   Bench-Capon, above n 57, 39.

60   Richard E Susskind, *Expert Systems in Law: A Jurisprudential Inquiry* (Clarendon Press, 1987) 114–15.

61   Philip Leith, 'The Rise and Fall of the Legal Expert System' (2010) 1(1) *European Journal of Law and Technology* <http://ejlt.org//article/view/14/1>.

62   Julius Stone, *Precedent and Law: Dynamics of Common Law Growth* (Butterworths, 1985) 63–74; Jeremy Waldron, 'Vagueness in Law and Language: Some Philosophical Issues' (1994) 82 *California Law Review* 509, 512–14; Laymen E Allen and Charles S Saxon, 'Analysis of the Logical Structure of Legal Rules by a Modernised and Formalised Version of Hohfeld Fundamental Legal Conceptions' in Antonio A Martino and Fiorenza Socci Natali (eds), *Automated Analysis of Legal Texts: Logic, Informatics, Law* (Elsevier, 1986) 385; Geoffrey Samuel, 'English Private Law: Old and New Thinking in the Taxonomy Debate' (2004) 24 *Oxford Journal of Legal Studies* 335, 362. See generally Ronald Stamper, 'Expert Systems – Lawyers Beware!' in Stuart S Nagel (ed), *Law, Decision-Making, and Microcomputers: Cross-National Perspectives* (Quorum Books, 1991) 19, 20.

63   On the challenges of interpreting legal rules and identifying exceptions, see generally Lon L Fuller, 'Positivism and Fidelity to Law – A Reply to Professor Hart' (1958) 71 *Harvard Law Review* 630, 661–9.

64   Anne von der Lieth Gardner, *An Artificial Intelligence Approach to Legal Reasoning* (MIT Press, 1987) 190.

Where these ideas have been more successful is in designing systems that can support rather than replace human decision-making by providing useful inputs or visualisations.[66] In this sense, currently available online legal databases and services are the modern equivalents of expert systems.[67] Similarly, there is some current research on tools to assist with the visualisation of evidence in complex investigations and litigation in order to enable traditional forms of reasoning about factual inferences for the benefit of police, legal practitioners and judges.[68] While lawyers were largely distrustful of the legal expert systems developed in the 1970s and 1980s,[69] particularly the possibility of unaccountable 'expert system' judges, they have embraced legal databases and other tools that preserve and enhance the ability for lawyers to analyse legal questions in traditional ways. Other professional groups and organisations have been much keener to embrace this type of technology in its originally intended form than lawyers. For example, expert systems have been employed by administrative agencies to automate decision-making around welfare.[70] The acceptability of automation is thus closely tied to the assumptions and priorities of the target users.

B   Police Information Systems: A Data-Oriented Approach to Police Decision-Making

Police information systems were developed in order to enable better informed law enforcement decision-making by providing police with accurate and complete information. Information gathering and processing is an essential part of police work, driven not only by crime control and internal management objectives, but also by the requirements of external agencies for risk management purposes.[71] Advances in computer technology have meant that police are collecting an increasingly broad range of data from both internal and external sources in textual, audiovisual and statistical formats. These data are

---

65   Uri J Schild, *Expert Systems and Case Law* (Ellis Horwood, 1992) 31–3.

66   Graham Greenleaf, 'Legal Expert Systems: Robot Lawyers? An Introduction to Knowledge-Based Applications to Law' (Paper presented at the Australian Legal Convention, Sydney, August 1989) <http://austlii.edu.au/cal/papers/robots89/>.

67   Richard Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford University Press, 2008) 16. See also comments in Graham Greenleaf, *Expert Systems Publications (The DataLex Project)* (30 December 2011) Austlii <http://www2.austlii.edu.au/~graham/expert_systems.html>.

68   See, eg, Floris J Bex et al, 'A Hybrid Formal Theory of Arguments, Stories and Criminal Evidence' (2010) 18 *Artificial Intelligence and the Law* 123, 125.

69   For an explanation of the limited relevance of expert systems to real world needs, see Philip Leith, 'The Application of AI to Law' (1988) 2 *AI & Society* 31.

70   See, eg, T J M Bench-Capon et al, 'Logic Programming for Large Scale Applications in Law: A Formalisation of Supplementary Benefit Legislation' in Thorne McCarty et al (eds), *Proceedings of the First International Conference on Artificial Intelligence and Law* (ACM Press, 1987) 190. See generally Citron, above n 55.

71   See Richard V Ericson and Clifford D Shearing, 'The Scientification of Police Work' in Gernot Böhme and Nico Stehr (eds), *The Knowledge Society* (D Reidel Publishing, 1986) 129; Ericson and Haggerty, above n 44.

used by police for a variety of operational (for example, checking suspicious vehicles or persons), investigative, and crime analytic purposes.[72] The attractions of computerised police information are many, as Chan suggests:

> New technologies promise improved effectiveness and efficiency in policing. … Computerised systems offer ready access, ease of use, speed of retrieval, and virtually limitless storage and analytical capacity for information processing. Advances in digitised image and video technologies have expanded the scope of what can be stored as information. These systems have also become increasingly portable, economical and mutually compatible. … Information technology … is especially suited for developing 'smart' policing strategies that are problem oriented, intelligence led and evidence based. Such technology is also ideal for making police officers and police organisations more self-regulating and more publicly accountable.[73]

However, early research has suggested that information technologies 'have been constrained by the traditional structure of policing and by the traditional role of the officer' and has had limited impact on police practices.[74] Later studies found that adoption of information technology was uneven and not always as intended.[75] Ericson and Haggerty's study of Canadian police organisations suggests that information technology has radically changed the structure and culture of policing, by restricting police discretion and making police activities more transparent and subject to scrutiny.[76] Chan's research found that the most successful use of information technology for proactive policing was in support of traditional law enforcement: the use of mobile data systems in police cars to check for outstanding traffic offence warrants.[77] The enthusiastic adoption of this technology is easily explained by its effectiveness, as evidenced by 'an exponential increase in the collection of fines as well as the imprisonment of fine defaulters.'[78] In terms of crime prevention or 'smart' policing, however, the impact of police information systems is less impressive. Some of the resistance is related to perceptions of police officers as to the inaccuracy or irrelevance of intelligence data for policing and law enforcement.[79]

That information technology can improve transparency of police decisions, police accountability and, by implication, the legitimacy of police organisations

---

72   See Chan, above n 40 for an early review of new technologies used by police organisations. Also see Peter K Manning, 'Information Technology and Police Work' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer, 2013) 2501.

73   Chan, above n 40, 655–6 (citations omitted).

74   Peter K Manning, 'Information Technologies and the Police' in Michael Tonry and Norval Morris (eds), *Modern Policing – Crime and Justice: A Review of Research Volume 15* (University of Chicago Press, 1992) 349, 350.

75   Chan, above n 40, 661–3.

76   Ericson and Haggerty, above n 44.

77   Chan, above n 40, 666.

78   Ibid.

79   Ibid 667; James Sheptycki, 'Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-Led Policing (2004) 1 *European Journal of Criminology* 307, 315–18, 323–4. See also Nina Cope, 'Crime Analysis: Principles and Practice' in Tim Newburn (ed), *Handbook of Policing* (Willan Publishing, 2003) 340, 357–8.

is an important reason for the popularity of its use for the management of the performance of local police commanders, the most famous example being the CompStat process pioneered in New York City. CompStat uses information technology to produce statistical profiles of arrests and crimes, which are presented at regular meetings of local commanders with top police executives. The 'grillings' of local commanders are a way of holding commanders accountable for the patterns of crime in their precincts.[80]

As in the case of legal expert systems, police information systems have been used to support traditional practices and approaches to decision-making. The picture is more complicated because policing interests are not uniform even within one organisation: police executives, local commanders, crime analysts, and operational officers working in different branches of police may perceive the costs and benefits of technology differently.

C Sentencing Databases: A Data-Oriented Approach to Judicial Decision-Making

Sentencing databases are an example of a decision-support system designed to assist judges in determining an appropriate sentence for criminal behaviour.[81] In this section, we limit discussion to the statistics component of the New South Wales Judicial Information Research System ('JIRS').[82] Sentencing databases treat precedents as data, storing them in a way that allows for the presentation of the ranges of sentences given out for different offences and circumstances; they are generally introduced in order to influence sentencing practices.

In New South Wales ('NSW'), the creation of the penalty statistics database in the original Sentencing Information System ('SIS') was motivated by concerns about disparities in sentencing, which had received significant media attention.[83] The goal of the system aligned with public concern about inconsistency in

---

80   John E Eck and Edward R Maguire, 'Have Changes in Policing Reduced Violent Crime? An Assessment of the Evidence' in Alfred Blumstein and Joel Wallman (eds), *The Crime Drop in America* (Cambridge University Press, 2000) 207, 230–1; Eli B Silverman, *NYPD Battles Crime: Innovative Strategies in Policing* (Northeastern University Press, 2001); David Dixon and Lisa Maher, 'Containment, Quality of Life and Crime Reduction: Policy Transfers in the Policing of a Heroin Market' in Tim Newburn and Richard Sparks (eds), *Criminal Justice and Political Cultures: National and International Dimensions of Crime Control* (Willan Publishing, 2003) 234. This was also implemented in NSW Police: see Hay Group Consulting Consortium, 'Qualitative and Strategic Audit of the Reform Process (QSARP) of the NSW Police Service: Report for Year 1 (March 1999 – March 2000)' (Police Integrity Commission, 2000); David Dixon, '"A Transformed Organisation"? The NSW Police Service since the Royal Commission' (2001) 13 *Current Issues in Criminal Justice* 203.

81   This is distinct from prescriptive or presumptive sentencing guidelines used in some US jurisdictions, see Janet B L Chan, 'A Computerised Sentencing Information System for NSW Courts' (1991) 7(3) *Computer Law and Practice* 137, 147.

82   See Judicial Commission of New South Wales, *Judicial Information Research System (JIRS)* <http://www.judcom.nsw.gov.au/research-and-sentencing/judicial-information-research-system-jirs>.

83   Chan, above n 81, 137–9.

punishment.[84] It was felt that if judges had easier access to historical sentencing patterns, inconsistency in sentencing outcomes might be reduced.[85] In particular, the use of particularised examples enabling bottom-up reasoning was considered more useful than preparation of a set of principles enabling top-down reasoning.[86] Other than the possibility of deletion of older cases, the database operated on the entire population of sentencing cases in the jurisdiction, rather than relying on sampling.[87] However, there were some situations where only a small set of relevant precedents would be relevant in a particular case.

The original SIS had four components, but the one of primary relevance here is the part of the database that collates statistics on past sentences, allowing a sentencer to discover the range of penalties imposed in past cases similar to one being considered. Similarity is defined by reference to the presence or absence of factors that were, at the time, both legally relevant to sentencing decisions and empirically related to the historical pattern of sentences.[88] Factors that were difficult to measure objectively, such as the degree of harm suffered by a victim, were excluded.[89]

The sentencing database has evolved over the years into the current JIRS. The original goal of achieving consistency in sentencing outcomes has shifted to a focus on achieving consistency in approach.[90] The approach of the Judicial Commission has always been to emphasise that '[t]he purpose of the system is

---

84   Public confusion and resentment about disparities in sentencing was analysed in a range of law reform commission inquiries: see, eg, Law Reform Commission, Interim Report No 15, Sentencing of Federal Offenders (AGPS, 1980). See also J J Spigelman, 'Consistency and Sentencing' (2008) 9 *Judicial Review* 45, 47: 'Nothing is more corrosive of public confidence in the administration of justice than a belief that criminal sentencing is primarily determined by which judge happens to hear the case.'

85   Chan, above n 81, 139.

86   Ibid.

87   Ibid, 148.

88   Ibid, 139. These include the offence and offender characteristics such as 'prior record, plea, liberty status at the time of the offence, age, whether there was one or more than one count of the principal offence, whether the sentence imposed took into account other admitted offences, and whether the offender was an individual or a corporation': Ivan Potas et al, 'Informing the Discretion: The Sentencing Information System of the Judicial Commission of New South Wales' (1998) 6 *International Journal of Law and Information Technology* 99, 113–14.

89   Chan, above n 81, 139.

90   Potas et al, above n 88. More generally, disparities in sentencing may be a result, not of judges giving different sentences where the same factors are held to be present, but rather different judicial perceptions of the facts and information before them: see, eg, John Hogarth, *Sentencing as a Human Process* (University of Toronto Press, 1971). In other words, different judicial attitudes may affect how they perceive 'raw facts' and, in particular, whether those facts imply the presence of particular factors. This has a greater impact on differences in sentencing than the decision as to what sentence is appropriate given the recognised presence of particular factors. Since a database can only map the correspondence between sets of factors and sentences given, and cannot affect how judges interpret facts, it may not have as significant an impact on consistency in sentencing outcomes as originally intended. The most a sentencing database can achieve is thus to ensure that sentencing decisions are based on the same approach, which takes account of past sentences in similar (perceived) contexts. For a general discussion of techniques of guidance: see Chan, above n 81.

not to curtail discretion, but to better inform it'.[91] Underlying this approach is the central assumption that sentencing discretion, while wide, is individualised within the constraints of statutory maximum penalties, the available sentencing options, aggravating or mitigating factors, common law principles of sentencing, and 'the principle that imprisonment is a sentence of last resort.'[92]

In NSW, the sentencing statistics database is used in a similar manner to case precedents. Judges consider the similarities and differences between a current offender and past sentencing cases. Judicial discretion and attention to the circumstances of the particular case remain central.[93] In that sense, like expert systems, the kinds of arguments that sentencing databases help people construct are *legal* arguments. While in theory, mathematical techniques could be employed to convert sentencing statistics into a best-fit weighted formula based on relevant factors, this is not the way the database is used in practice. This does not imply that the database has had no influence on narratives around punishment, or that it does not favour some punishment rationales over others.[94] But it does mean that the sentencing database influences sentencing outcomes by enhancing judicial access to a particular kind of *legally relevant* information. It does not replace legal argument with statistical reasoning.

The relative acceptance of the sentencing statistics database by NSW courts owes a great deal to this embrace of reasoning and processes that sentencers would regard as legitimate.[95] Moreover, the source, method of collating and the use of this data are open and transparent, while sentencing decisions are accountable in open court and subject to appeals. These points are summarised by Potas in terms of the '[p]rinciples of accountability':

> although judicial officers are free to decide cases 'without fear or favour', they are accountable to the law and lose legitimacy if they do not apply it. …
>
> Amongst the most important accountability principles are the requirements that a court give reasons for sentence, that the sentencing hearing is conducted in open court and that parties may appeal (or seek leave to appeal) against sentence on the ground that the judge or magistrate 'got it wrong'. …
>
> The cards are on the table; there are no hidden agendas. What is done in a particular case can be understood by reference to the reasons given. The sentence imposed can be compared openly with other cases, with the general pattern of sentences reflected in the statistics and of course with the penalties expressed in the legislation. A reference to the statistics in the remarks on sentence adds to the

91   Potas et al, above n 88, 99. This is also explicitly stated in the *Judicial Officers Act 1986* (NSW) ss 8(1)–(2).

92   Ivan Potas, 'The Use and Limitations of Sentencing Statistics' (2004) 31 *Sentencing Trends & Issues* <http://www.judcom.nsw.gov.au/publications/st/st31>. See also *Crimes (Sentencing Procedure) Act 1999* (NSW) s 5(1).

93   Eg, *DPP (Cth) v De La Rosa* (2010) 79 NSWLR 1, 70–1 [304]–[305] (Simpson J).

94   David Tait, 'Judges and Jukeboxes: Sentencing Information Systems in the Courtroom' (1998) 6 *International Journal of Law and Information Technology* 167, 174.

95   George Zdenkowski, 'Limiting Sentencing Discretion: Has There Been a Paradigm Shift?' (2000) 12 *Current Issues in Criminal Justice* 58.

justification and transparency of the decision and this in turn facilitates the appeal process; the latter itself is governed by the same considerations.[96]

Thus, sentencing statistics databases are designed to assist people with legal decisions by providing information. These databases are no more sophisticated than a computerised library, with a facility to search for like cases and display statistical patterns of past sentences. They provide information that fits in with, and preserves, traditional approaches to the exercise of sentencing discretion. The Australian Law Reform Commission has noted that the establishment of a national database had 'overwhelming support from government and non-government organisations, Commonwealth prosecuting authorities, judicial officers, legal practitioners, federal offenders and academics.'[97] Their acceptance, particularly within the judiciary, lies in both the fit with judicial practice and the effectiveness and perceived appropriateness of their use.

D   What Is New about Big Data?

'[A] change of scale leads to a change of state. … [This transformation] presents an entirely new menace: penalties based on propensities.'[98]

In evaluating the effectiveness and acceptability of a new technology, it is necessary to isolate the features that define it. As can be seen from Part II, big data analytics is an empirical technique. This differentiates it from legal expert systems that were based on traditional doctrinal approaches to reasoning, although both rely on 'rules' to draw inferences.

Like many earlier empirical approaches, big data analytics speaks the language of probability, enhancing decision-making by estimating the likelihood that particular facts are or will be true. This approach can be distinguished from the primary uses made of earlier data-driven tools such as police information systems and sentencing databases. While information systems and sentencing databases offered some potential for statistical analysis, they were primarily used as means of locating particular relevant data points, such as the existence of outstanding warrants or the sentences given in particular legally analogous precedents. Big data has a very different focus – there is a recognition that individual data points may be unreliable and accuracy of datasets is often sacrificed in favour of volume. Insights are gained not from the ability to recall relevant data points, but from the ability to identify correlations and patterns across a large number of data points. While there was some potential for this in earlier technologies, that potential was largely ignored by police and judicial users.

From a technical perspective, the techniques used in the analysis of big data draw from older machine learning techniques. All that is new is the size of

---

96   Potas, above n 92.

97   Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, Report No 103 (2006) 529 [21.15].

98   Mayer-Schönberger and Cukier, above n 2, 151.

datasets being analysed. However, this technical fact has other implications. First, and most obviously, the use of larger datasets makes it possible to detect correlations and patterns that might otherwise have been missed. Conclusions that would not be statistically justified if based on a small or moderate sample can be made with reference to a sufficiently large dataset. Secondly, big data analytics is less transparent than empirical analysis based on smaller datasets. Technical expertise may not be required to realise that statistical conclusions purportedly drawn from a small, easily grasped, dataset must be false. However, in the case of big data, access to the datasets and unassisted human understanding of what they may (or may not) signify, are both problematic. Drawing on both of these differences, there is a greater potential for mythological thinking about conclusions drawn from big data compared to earlier empirical techniques. The same incomprehensibility that reduces transparency can magnify the sense of awe generated among those without the technical ability to understand the limitations of different techniques. The capacity of big data analytics to make unexpected predictions with a high degree of accuracy in a variety of different fields further fuels its almost magical aura.

The challenge of big data is thus not so much that it involves a new form of reasoning, but rather that it provides a significant enhancement to empirical techniques that gives rise to an aura of invulnerability that is also more difficult for non-experts to understand and evaluate. Big data techniques are both less intuitive and more powerful than older empirical techniques. While limited use was made of the statistical features of police information systems and the sentencing database, it is not yet known whether the professional reaction to big data will be the same. In other words, will the mystique and power of big data tools lead to greater use of empirical and statistical reasoning in legal and law enforcement decision-making?

V   EVALUATING BIG DATA ANALYTICS FOR LEGAL AND POLICING DECISIONS

The idea that big data analytics might help with legal decision-making has generated both enthusiasm and fear.[99] On the negative side are dystopian scenarios, such as portrayed in *Minority Report*.[100] On the positive side, better prediction may save legal costs associated with dispute resolution and enable more efficient deployment of police and correctional resources.[101] Such efficiencies lead some to believe that quantitative legal prediction is coming

---

99   See Daniel Martin Katz, 'Quantitative Legal Prediction – or – How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry' (2013) 62 *Emory Law Journal* 909; Milgram, above n 7. Cf Harcourt, above n 9.

100   This is a reference to the movie *Minority Report* (Directed by Steven Spielberg, Cruise/Wagner Productions, 2002), loosely based on Philip K Dick, *The Minority Report* (King-Size Publications, 1956).

101   See, eg, Katz, above n 99; Milgram, above n 7.

'whether you like it or not' and that law students and lawyers are well-advised to learn the necessary skills.[102]

However, in our view, no particular use of these tools is inevitable. What is ultimately implemented will depend on professional, organisational and public responses to particular techniques. In light of the lack of literacy in the techniques involved among legal professionals, it is possible that new techniques will be embraced as an external given, not understood but assumed to be accurate. It is also possible that legal and police professionals may resist techniques that they do not understand. It is only based on understanding that more nuanced and desirable responses become likely.

In order to facilitate this, and in order to understand the challenge these techniques may pose to professional and social values, we evaluate big data analytics using the criteria identified in Part III, namely effectiveness, acceptability and appropriateness.

A   Effectiveness

In the case of technologies that can be employed in decision-making, such as big data analytics, effectiveness is closely related to accuracy. If the information provided by big data analytics is wrong or misleading, perhaps due to calculation errors or distorted description of results, then it is simply unhelpful. The accuracy of inferences drawn from big data is highly contingent on the methods used in generating them, whether traditional statistics or machine learning, and the explicit and implicit assumptions made in employing those techniques. While one could base decisions on false or misunderstood information, for example if one were hoodwinked into accepting its accuracy, this is unlikely to be sustained over the longer term.

In the realms of pure calculation, big data *can* perform well.[103] For example, one study compared a classification tree machine learning approach with the predictions of elite lawyers and law professors as to the votes of individual US Supreme Court Justices in future cases.[104] The machine was not working on its own, but required humans to input specific information, such as the ideological direction of the lower court ruling. The classification tree won, with 75 per cent success compared to 59 per cent. Success stories in the realms of prediction are likely to flourish. As data becomes 'bigger', more experience can be captured than a single human mind might be able to consume. As analytic techniques develop, better algorithms will be able to make sense of larger and more complex datasets, albeit with only probabilistic conclusions. Limits of historical empirical

---

102   Katz, above n 99, 912.
103   See generally Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2011).
104   See Theodore W Ruger et al, 'The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decision-Making' (2004) 104 *Columbia Law Review* 1150.

techniques, such as the potential biasing effect of small samples, can be overcome by analysing *all* data.[105]

The fact that big data will have successes does not mean, however, that big data analysis is always successful. Even in the case in 'small data' analysis, statistical errors are common. As data size increases, so does the potential for mistakes. There is insufficient space here to enumerate the types of mistakes which can occur, each of which would require an explanation referencing the rules of statistical inference. Many common errors have been identified by others.[106] To give an example of the type of error we are talking about, consider a large dataset associated with an entire population (N = all), such as the prison population in Australia or the twitterverse. It would be inappropriate to draw conclusions from those datasets as if they are representative of 'all criminal offenders' or 'community opinion'.[107] Another type of error occurs when data is missing, so that correlations drawn have no causal foundation. For example, large fires are associated with both significant damage and escalated response (more fire engines at the scene). If one had data that captured both the extent of damage and the scope of the response (but not the size of the fire), one might wrongly deduce that more fire engines at a scene leads to greater damage from the fire, an absurd conclusion.[108]

Beyond statistical fallacies, human biases are introduced into the analysis of data. As noted above in relation to machine learning, these are impossible to avoid. It is a human who identifies and selects the data to be analysed (which may have varying levels of accuracy) and chooses the algorithm to be employed. Some of the time, a human also selects the attributes and variables that are treated as relevant.[109] In the case of big data, additional biases result from the process of 'cleaning' data. Errors in datasets and statistical outliers are often 'fixed' prior to analysis. Removing statistical outliers may bias conclusions towards those that assume lower rates of variability than occur naturally.[110] Further, even well-structured cleaning techniques are often probability based, for example two individuals in distinct datasets might be treated as being the same person if similarities in their names or other characteristics make this statistically likely.

Big data analytics may mislead rather than aid decision-makers if it is assumed that the numbers simply 'speak for themselves'. Like inferences drawn on other bases, they require careful interpretation.[111] In particular, it is important

---

105 Hunter, above n 27, 143–4 (discussing the problems of relying on small datasets).
106 See, eg, Richard Berk, *Criminal Justice Forecasts of Risk: A Machine Learning Approach* (Springer, 2012).
107 Eg, boyd and Crawford, above n 38, 668–70.
108 The authors are grateful to Michael Smithson for this example.
109 David Bollier, 'The Promise and Peril of Big Data' (Communications and Society Program, Aspen Institute, 2010) 15.
110 Ibid 8.
111 Ramsay, above n 37, 62.

to understand assumptions made in the analytic process (including around choice of datasets and algorithms) in order to craft appropriate inferences. There is an additional risk that translation errors may occur when different individuals or teams contribute different elements as, for example, where different people or groups are involved in data collection, construction of the algorithm used to analyse the data and using outputs for decision-making. The first group may understand the limits of the dataset (including gaps in collecting the data and biases in cleaning the data), the second group the biases and estimates introduced through choice of algorithm and the third group the nature of the decision to be made. Proper communication of the nature and limits of inferences drawn, at all levels, is essential in order to ensure that non-statisticians interpret the results correctly.[112] There is also a need for careful employment of visualisations used to derive and explain inferences among users – while visualisations can be a valuable means of observing and understanding patterns in data, they can also be misleading.

None of these calculation errors, biases and misinterpretation are *necessarily* problematic in every big data analysis. It is possible to avoid statistical mistakes, stating conclusions in a form that takes account of biases introduced in the process and ensure clear communication and informed interpretation of results. It is also possible to verify statistical predictions and correlations through proper testing on new data before allowing these to influence decisions.

Statistical conclusions can form the basis for a rational approach to legal and law enforcement decision-making. For example, a lawyer must decide whether or not a document is discoverable. Data analytic techniques might be used to show all the documents that have more than a fixed probability of being discoverable, with those documents being analysed by a human. Similarly, knowing the probability that a person charged with an offence will turn up for a hearing, or the probability that a current offender will reoffend, can be usefully factored into decisions around bail and parole. Inferences drawn in police use of big data analytics are also useful in law enforcement decision-making, including in the performance of traditional functions. For example, datasets might be combined to identify and locate a perpetrator based on known characteristics (for example, by using facial recognition software or data matching), or to calculate the probability that a person being observed by police is involved in a criminal act (derived from observable characteristics and behaviours as well as contextual factors such as location) as a basis for conducting a search.[113]

There are some barriers to effectiveness that are independent of accuracy, such as the problem of feedback, where action taken on the basis of analytic

---

112   Similar issues exist in ensuring juries draw appropriate inferences from DNA evidence: see, eg, Stephanie Dartnall and Jane Goodman-Delahunty, 'Enhancing Juror Understanding of Probabilistic DNA Evidence' (2006) 38 *Australian Journal of Forensic Sciences* 85.

113   The legality of such searches is a separate question, beyond the scope of this article. In the United States, see Andrew Guthrie Ferguson, 'Predictive Policing and Reasonable Suspicion' (2012) 62 *Emory Law Journal* 259.

techniques leads to changed behaviour. While feedback issues arise in many other contexts, for example changes in behaviour to (narrowly) avoid reporting requirements, they are particularly important where decisions are based on non-causally linked correlations. To the extent people are aware of decisions being made that affect them based on correlations, they may change their behaviour.[114] For example, if police were to find a correlation between crime rates and tattoos, people may choose not to get tattoos in order to avoid enhanced suspicion. While the (purely hypothetical) correlation between tattoos and criminal activity may exist prior to police action, the change in behaviour to which the police action leads results in less tattoos but not less criminal activity. In the criminal context, one can minimise feedback problems only by reducing transparency, so that people do not know why they are targeted by police.[115]

Similar feedback applies in non-criminal contexts. There would be feedback effects if big data predictions were to become an important component of decision-making about the commencement of proceedings, the claims pursued, the settlement offers made and accepted, and the design of legal transactions.[116] The 'shadow of the law' in which decisions and negotiations take place could well extend beyond doctrinal analysis[117] that seeks to understand the law promulgated by legislatures and judges, to predictions made by analysing those same statutes and judgments as data using statistical and learning techniques. The data would become skewed over time – taking cases out of the system through settlement limits legal development and the creation of new precedents, biasing the sample of cases that ultimately make it to court.[118] A skewed sample of litigated cases changes the dataset on which predictions are based. Further, settlements themselves often become known 'data points' and influence both future settlements and future damages awards.[119] Relying on past data, including past settlements, when making settlement decisions creates a feedback loop so that an initial bias in favour of plaintiffs or defendants is perpetuated. This is more problematic for empirical techniques compared to doctrinal techniques, since for the latter a case is only relevant as precedent for normatively similar cases. Pure predictive techniques do not analyse the cases in the same way, they merely search for correlations, and assume that the training data is representative. To the extent that the legal norms themselves become less important and relevant

---

114   Mireille Hildebrandt, 'Who Needs Stories If You Can Get the Data? ISPs in the Era of Big Number Crunching' (2011) 24 *Philosophy & Technology* 371.

115   Ibid.

116   See generally Dru Stevenson and Nicholas J Wagoner, 'Bargaining in the Shadow of Big Data' (2014) forthcoming *Florida Law Review* (copy on file with author) 44 <http://ssrn.com/abstract=2325137>.

117   Robert H Mnookin and Lewis Kornhauser, 'Bargaining in the Shadow of the Law: The Case of Divorce' (1979) 88 *Yale Law Journal* 950, 959–77.

118   Donald Wittman, 'Dispute Resolution, Bargaining, and the Selection of Cases for Trial: A Study of the Generation of Biased and Unbiased Data' (1988) 17 *Journal of Legal Studies* 313; Rex R Perschbacher and Debra Lyn Bassett, 'The End of Law' (2004) 84 *Boston University Law Review* 1.

119   Ben Depoorter, 'Law in the Shadow of Bargaining: The Feedback Effect of Civil Settlements' (2010) 95 *Cornell Law Review* 957, 974 ff.

outside the courtroom, there are consequences for the role of law in society more broadly.[120] In practice, few cases are litigated, but transactions and settlements are common. Changing the rules of the latter game, working statistically rather than normatively, changes many decisions in fundamental ways.

The first key to legal and law enforcement communities being interested in big data analytics is thus the potential for accurate predictions about future conduct based on the presence or absence of correlative factors. While big data offers a high degree of potential predictive value, this depends on data quality (which can be lower for large datasets than for smaller ones, but it remains important), the success of algorithmic approaches (in theory and in practice), the precision with which conclusions are stated and proper testing of conclusions against data independent of the 'training data'. As we have demonstrated above, faith in the apparent rationality and objectivity of big data is often misplaced. Actual performance of analytic approaches in areas such as electronic discovery has been variable (depending on methodology and the documents being examined).[121] In practice, it is not only important that the numbers are 'right' (and sometimes mistakes are made), but that their meaning is explained or visualised in a way that enables an accurate and precise understanding by non-statisticians. Subjectivities and biases need to be made explicit if inferences drawn in non-statistical contexts (such as law and law enforcement) are to be reliable. Accuracy is certainly possible, if difficult to achieve. Ultimately, effectiveness can be measured (in part) by reference to the effectiveness of decisions based on inferences derived from analytics with reference to criteria such as crime prevention outcomes.[122] This will need continuous monitoring due to the potential for feedback effects.

Ineffectiveness in the context of big data does not only mean that decisions will be 'wrong', it also means that decisions may be unfair. If a person's liberty, for example, is taken away based on inaccurate statistical correlations, then that is both unhelpful and unjust.

B   Acceptability

As foreshadowed, the acceptability of big data techniques within legal and policing professions and organisations is difficult to predict. Much depends how legal and justice practitioners perceive the capability, costs and benefits of using this technology – that is, their technological frames – which can vary according to individual attitudes, organisational factors, or network effects (once some individuals or organisations experiment with the technology, others may be prepared to try). Acceptability will in particular hinge on perceived effectiveness, including the link between effectiveness and just outcomes.

---

120   Perschbacher and Bassett, above n 118.
121   Pace and Zakaras, above n 6, 62–6.
122   See, eg, Greg Ridgeway, 'Linking Prediction and Prevention' (2013) 12 *Criminology & Public Policy* 545.

While big data analytics can support traditional policing practices, it has great potential for turning reactive policing into various 'smart' policing approaches such as problem-oriented, intelligence-led and hotspot policing.[123] For example, some criminologists have urged increased use of such 'predictive policing' tools.[124] The focus of 'predictive policing' is not the solution of any particular crime or apprehension of any particular offender but rather ensuring crime reduction and safer communities through crime prediction.[125] A variety of analytical models are already being used for predicting crime: geographic information systems ('GIS's) from simple crime-mapping to sophisticated regression and neural network strategies, and increasing reliance on the 'random forest' algorithm to predict the probability of crime occurring in a particular place tomorrow.[126] Yet predictive models have not led to many practical applications in policing practice. One 'success story' relates to the Richmond Police Department which in 2003 used predictive crime analysis, data mining and GIS techniques to inform their deployment of police officers. The use of predictive tools revealed 'hidden patterns and relationships'[127] and 'unanticipated factors' which purportedly 'added value to (1) deployment, (2) tactical crime analysis, (3) behavioural analysis of violent crime, and (4) officer safety.'[128] In spite of showing 'promise', predictive policing was discontinued in Richmond when a new police administration took over, and 'more traditional' policing strategies were once again employed.[129] Another example of the application of predictive models to policing was the field testing of a mathematical model based on 'self-exciting point processes' and repeat victimisation theory to determine police patrol strategies at the Los Angeles and the Santa Cruz Police Departments: preliminary findings showed a drop in non-violent crime in the experimental areas.[130] According to media reports, Chicago is also running a predictive policing program that targets both individuals and locations,[131] while Detroit is using big data analytics to identify what drives crime and understand the structure of criminal organisations.[132] The wider adoption of

---

123 See Herman Goldstein, *Problem-Oriented Policing* (McGraw-Hill, 1990); Lawrence W Sherman, Patrick R Gartin and Michael E Buerger, 'Hotspots of Predatory Crime: Routine Activities and the Criminology of Place' (1989) 27 *Criminology* 27; Jerry Ratcliffe, *Intelligence-Led Policing* (Willan Publishing, 2008).

124 See, eg, Richard A Berk and Justin Bleich, 'Statistical Procedures for Forecasting Criminal Behaviour: A Comparative Assessment' (2013) 12 *Criminology & Public Policy* 513.

125 Uchida, above n 10, 3871.

126 Ibid 3874–6.

127 Ibid 3876, quoting Colleen McCue and Andre Parker, 'Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis' (2003) 70(10) *Police Chief* 115.

128 Uchida, above n 10, 3876.

129 Ibid.

130 Ibid, 3877

131 Matt Stroud, *The Minority Report: Chicago's New Police Computer Predicts Crimes, but Is It Racist?* (19 February 2014) The Verge <http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist>.

132 Joe Nicholson, *Detroit Law Enforcement's Secret Weapon: Big Data Analytics* (16 May 2014) VB News <http://venturebeat.com/2014/05/16/detroit-law-enforcements-secret-weapon-big-data-analytics/>.

big data analytics by police remains to be seen. If previous research on the use of policing databases is any guide (see Part IV), the acceptance of big data technology is likely to be uneven: police executives, commanders and crime analysts will be attracted to its promise of improved effectiveness for policing, while operational officers – initially, at least – will 'cherry pick' and adopt aspects of technology that suit their policing style.

Similarly, in spite of the capacity of big data to enhance decision-making, legal professionals are also likely to be reluctant to replace traditional doctrinal approaches to reasoning with data-driven or automated methods. The history of legal expert systems and sentencing databases suggests that technologies were accepted mostly as tools for assisting with traditional doctrinal reasoning. In the case of legal expert systems, the use of automated decision-making was largely confined to routine decision-making within administrative agencies and rarely employed by legal professionals. In the case of sentencing databases, where the consistency of statistical outcomes was initially intended, this was largely replaced by a 'consistency of approach' methodology, which fits more closely with sentencing principles and judicial reasoning. One might therefore anticipate a similar reluctance to embrace decision-making that relies primarily on inferences drawn from big data analytics. Even in the area of electronic discovery, where the application of analytic techniques is relatively straightforward, the process is not widely used due largely to concerns about effectiveness as well as professional inertia and risk aversion.[133]

There are thus significant challenges for the diffusion of big data techniques in legal and law enforcement contexts. The technological frame in which data analytics operates runs counter to traditional ways of using information to make decisions. On the other hand, there is significant, mostly positive, hype around big data in the business, technical, political and national security communities. Much may depend on the success of early adopters, both legal and law enforcement, in the US.

C   Appropriateness

As discussed in Part III, the real and perceived appropriateness of big data techniques in legal and law enforcement decision-making is likely to hinge on its alignment with legal rules, and the extent to which it preserves accountability and its transparency, both to its users and to the general community. It will also hinge on effectiveness, to the extent that ineffective use of data leads to unjust outcomes.

1   Legality

Some uses of big data may run afoul of well-established legal norms. This is most obvious when considering the possibility that big data might be used in

---

133   Pace and Zakaras, above n 6, 71–83.

guiding judicial discretion in contexts such as bail and sentencing. In traditional legal reasoning, and even legal expert systems, factors taken into account are chosen because of their normative importance. Where empirical data is used, as is the case for big data analytics, factors identified are those that correlate with particular outcomes, not those that are normatively or even necessarily causally relevant. There are strong reasons for linking judicial decisions with legally relevant, and not merely statistically relevant, factors. It is arguably unjust to take account of a factor such as shoe size, even if this were statistically relevant. This was done explicitly in designing a sentencing database for judges in NSW. It can be done in other contexts (it is possible to ignore non-legally relevant correlations), but only where analytic techniques are made transparent. As was the case with legal expert systems, transparency is crucial to ensure that the legal norms used are both accurate and able to be updated.

In the case of predictive policing, concern hinges around a fear that civil liberties may be eroded in a *Minority Report*-like policing strategy that focuses on citizens before they have committed crimes.[134] While such an extreme example is unlikely, using data analytics to alter policing practices is still problematic. Profiling of geographical areas and communities presents dangers that whole areas or communities are stigmatised and initial statistical correlations eventually become a self-fulfilling prophecy.[135] This not only perpetuates stereotypes but can ironically increase the rate of crime.[136] Discrimination is again a risk, particularly if law enforcement are able to shift accountability for decisions to target particular communities onto a non-transparent algorithm.

Decisions based on discriminatory grounds are problematic in themselves. The point here is that *even if* there is a correlation between particular events and certain characteristics (such as race), that does not make it appropriate to discriminate on the grounds of race itself. There are things we are rightly unwilling to use as proxies. The problem with big data is that the proxies employed by an algorithm may not be transparent. Further, as is the case in legal rules, relevant factors may themselves correlate with impermissible ones, as where there is a known correlation between characteristic X and feature Y and a hidden correlation between feature Y and race Z. Using feature Y may seem racially neutral, but in practice it will operate in a discriminatory way. We have laws against particular types of discrimination for good reasons. It is illegal to discriminate against someone because of their race *even if* such characteristics are correlated with undesirable traits. Where discrimination is explicit, it is possible to complain. The difficulty with correlative analysis is that there are many (correlative) proxies for race and gender.[137] This means that, absent transparency, it is not always obvious when a machine learns to discriminate.

---

134   See discussion in Uchida, above n 10, 3878.

135   Harcourt, above n 9*, 33.

136   Profiling may increase offending where the profiled group is less likely to change its behaviour based on levels of policing and punishment compared to the non-profiled group: Ibid 24.

137   Ian Ayres, *Super Crunchers: How Anything Can Be Predicted* (John Murray, 2007) 174–5.

The problem of discrimination arose in the Virginia example introduced in Part I. A decision to release on parole those who commit sexual offences against girls earlier than those who commit sexual offences against boys raises fundamental issues beyond accurate reflection of statistical dangerousness. There are real questions about messages sent or perceived more broadly about relative criminality of the same offence committed against victims of different genders. There are also practical risks in that, statistically, the differential parole policy places girls at greater risk than boys of being the victim of a repeat sexual offender. While this may seem bizarre, particularly assuming accurate rates of reoffending are relied on in allocating points, it is nevertheless true. For reasons articulated by Harcourt, while those who abuse girls are less likely to reoffend, they are more likely to be released following a single conviction, so a lower proportion of them will be incarcerated at any one time (other things being equal).[138] The result is a community that contains a higher ratio of girl abusers to boy abusers than would exist had the parole policy not been biased. Depending on the numbers involved, this can overcompensate for the fact that those who abuse boys are more likely to reoffend, and in fact be overly protective of boys relative to girls. By skewing protection according to gender, a generally impermissible ground, the policy can operate in a discriminatory way (both in practice and symbolically) even where it is based on sound statistics. To pretend that these issues do not exist because of a statistical correlation ignores the broader issues around the legitimacy and acceptability of discriminatory policies.

The Virginia example predates modern big data techniques. It deployed a relatively simple 'points' system, based on empirical observation, for determining who would be granted parole. The simplicity both decreased precision (it only identified a few relevant features) and enhanced transparency – it was easy to see that those who abused boys would be required to spend longer in prison. Big data changes both of these features. One can enhance precision, discriminating on the basis of a broader range of factors due to the ability to spot more obscure correlations between repeat offending and particular traits. On the other hand, moving beyond the points system to a more refined model may make it more difficult to detect discrimination where it does occur.

These problems can be avoided. One can design systems to ensure that they avoid taking features such as race, or characteristics that correlate with race, into account. Alternatively, one can choose to use learning algorithms that only look for correlations with legally relevant factors. While these may still correlate with

---

138   Harcourt, above n 9, 10–15, 147–60, 168–9.

a feature such as race, one is no worse off than with traditional doctrinal reasoning or a sentencing database such as the one in NSW.[139]

Of course, discrimination can occur even in ordinary intuitive reasoning. Given the non-transparency of the human mind, the only way to deter discriminatory reasoning is by relying on accountability in decision-making. Many decision-makers are required to give reasons, either within their organisation, or publicly. While this does not avoid discrimination, it does reduce it. There is thus a difference between discriminatory reasoning based on human prejudice and discriminatory reasoning based on 'objective' statistics-based reasoning, and it lies in human accountability.

2 Accountability

The use of big data techniques to make public decisions requires accountability mechanisms to be acceptable both within particular institutions and in society more broadly. As explained above in Part III(C), accountability is an important value within the legal profession, the judiciary and the police. Such professionals may be uneasy with predictive tools that function like a 'black box', especially if they come up with 'hidden patterns and relationships' and 'unanticipated factors',[140] where these may not make sense with reference to their professional expertise and experience. In other words, predictive tools can reduce the accountability of decisions, strategies and actions.

The lack of human accountability inherent in decisions based on algorithms limits their use in some legal contexts. Being based on correlation, statistical techniques fail to provide a normative basis for future decision-making or capture the kinds of reasoning in which judges and many other public decision-makers must engage.[141] A person can be told that that they are not going to be released on parole because of their history of violent crime, but correlative statements do not necessarily provide a similarly sufficient explanation unless the causal link can

---

139 In some cases, race does correlate with a legally relevant factor, including those itemised in sentencing databases. See, eg, US research such as Ronald A Farrell and Victoria Lynn Swigert, 'Prior Offence Record as a Self-Fulfilling Prophecy' (1978) 12 *Law & Society Review* 437; Cassia Spohn, John Gruhl and Susan Welch, 'The Effect of Race on Sentencing: A Re-examination of an Unsettled Question' (1982) 16 *Law & Society Review* 71. For Australian research on the relationship between Aboriginality and prior record among young offenders, see Garth Luke and Chris Cunneen, *Aboriginal Over-Representation and Discretionary Decisions in the NSW Juvenile Justice System* (Juvenile Justice Advisory Council of NSW, 1995). See also Christine E W Bond, Samantha Jeffries and Don Weatherburn, 'How Much Time? Indigenous Status and the Sentenced Imprisonment Term Decision in New South Wales' (2011) 44 *Australian & New Zealand Journal of Criminology* 272, who found that while Indigenous defendants in New South Wales had more serious prior records than non-Indigenous defendants, more extensive criminal histories had inconsistent effects on terms of imprisonment (longer in the lower courts but shorter in the higher courts); their analysis found no sentencing disparity between Indigenous and non-Indigenous offenders in the higher courts and a reduced length of sentence for Indigenous offenders in the lower courts, when other factors such as demographics, plea, and current and prior criminality were taken into account.
140 Uchida, above n 10, 3876.
141 Hunter, above n 27.

be intuitively grasped. The problem is compounded in the absence of transparency in the datasets and methods used to derive the correlation. The implementation of predictive policing practices may reduce accountability for strategic decisions, particularly where there is a lack of transparency about the data used, the calculations performed and the way this influences practice. Public accountability is less crucial where big data techniques are part of private decision-making, other than in the sense that legal practitioners are accountable to their clients for poor advice and, in the context of electronic discovery, to the court.

In a legal and law enforcement context, accountability is not solely about formal responsibility, whether to clients, superiors or the broader community. There is an important human element – it matters that particular decisions are made by *people* who take responsibility for the decisions they make. Even if a legal expert system could be made highly effective and accurate, it was never seriously contemplated as a replacement for human judges. As Dalton and Thatcher write in a completely different context, '[a]s the fullness of human experience in the world is reduced to a sequence of bytes, we should not limit our concern to how much better those bytes function vis-à-vis their counterparts.'[142] While it may often be useful and appropriate to use big data techniques as an input into a human decision-making process, automating this process so as to remove or minimise the human element from high-stakes legal and law enforcement decisions will likely be both unacceptable to professional communities and seen as inappropriate more broadly.[143]

3   Transparency

Of the tools examined in this article, big data is the least transparent, at least to lawyers and police. Few lawyers are trained to understand what lies inside the black box. The stories about the mysterious accuracy of big data, promulgated through both the media and scholarship, are increasingly well-known. While larger datasets may enhance accuracy of predictions, they are also harder to access. Similarly, more complex techniques and algorithms may be more effective than traditional statistical techniques, but they are also harder to interpret and understand.

Because of the lack of reasons for a particular inference, some inferences will be non-intuitive or hard to explain. While legal conclusions can be rebutted with careful argument that counters or undermines the premises of one's opponent, big data conclusions cannot be dismissed 'merely' because they seem arbitrary or lack a logical basis. The only way to counter inferences is to understand (and

---

142   Craig Dalton and Jim Thatcher, *What Does a Critical Data Studies Look Like, and Why Do We Care? Seven Points for a Critical Approach to 'Big Data'*, Society and Space Open Site <http://societyand space.com/material/commentaries/craig-dalton-and-jim-thatcher-what-does-a-critical-data-studies-look-like-and-why-do-we-care-seven-points-for-a-critical-approach-to-big-data>.

143   See generally O'Malley, above n 15, on telemetric policing.

critique) the data and methods used to derive them in order to show that they are erroneous or overstated.[144] Doing this requires access to the data, the analytic methods used in the initial calculation, the processing power to duplicate it and the expertise to understand it.[145]

For some, the lack of transparency is irrelevant. It has been suggested that judges do not need to understand the reasons for the forecasts on which they base their decisions.[146] According to this view, even if decisions were made based on an offender's shoe size, so long as shoe size correlated statistically with the relevant behaviour (such as reoffending or breaking bail), this should be treated as a relevant factor in legal decision-making. This ignores the extent to which taking into account non-relevant factors is unjust.

The law's traditional concern with natural justice means that transparency is crucial. Some have argued for due process or natural justice requirements whenever state actions are based on predictive or opaque techniques.[147] Suggestions include a requirement for notice that predictive analytics will be used in a decision affecting a person, for a right to be heard in response, for transparency in the methods used to make predictions, for regular audits of the accuracy of the predictions made, for a right to check the accuracy of calculations, and for the right to an impartial adjudicator on questions around undue reliance on data.[148]

Beyond issues of natural justice, transparency is essential to society's evaluation of public decision-making. There are significant problems with Virginia's formula for determining bail for sex offenders. However, we are only able to critique that system because of its transparency. Policymakers and the community know that sex offenders spent different lengths of time in prison depending on the sex of the victim since the points system was public. The same is true for the pre-trial system developed by the Arnold Foundation. However, big data risks obfuscating the factors that are ultimately taken into account. It is possible to deploy machine learning techniques that hide the processes used to make decisions and predictions or present them in a way that is difficult for untrained people to interpret.

In a policing context, such secrecy can be seen as desirable. As explained earlier, there are concerns about feedback effects where offenders avoid correlated behaviour while still committing crimes, thus partially negating the effectiveness of 'predictive policing' programs.[149] Secrecy can be a solution.

---

144   Cf Citron, above n 55, 1305–6, 1308–9 on audit trails and open source for government decision systems.
145   See Mark Andrejevic, 'Surveillance in the Big Data Era' in Kenneth D Pimple (ed), *Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards* (Springer, 2014) 55, 60, 68 (describing the need for access to data and explanations of analytics underlying decisions). We believe that the four elements described meet this need.
146   Berk and Bleich, above n 124, 517.
147   Kate Crawford and Jason Schultz, 'Big Data and Due Process: Towards a Framework to Redress Predictive Privacy Harms' (2014) 55 *Boston College Law Review* 93; Citron, above n 55.
148   Crawford and Schultz, above n 147; Citron, above n 55.
149   See also Tal Z Zarsky, 'Transparent Predictions' [2013] *University of Illinois Law Review* 1503.

However, there are still reasons to be concerned about a lack of transparency in a policing context. As a society, we may be uncomfortable with the idea that people are unable to resist negative conclusions being drawn about them, either by changing their actions or by undermining the inferences (perhaps by challenging the methods used).[150] There may be broader harms, including psychological harms, caused by non-transparency in these circumstances, even where the inferences are quantitatively accurate. Non-transparency can also enable and obscure illegal practices.

Transparency is an important value, both for its own sake, and in its link with ensuring effectiveness, legality and accountability. It is also problematic, and can generate unintended consequences, such as feedback loops, that undermine the effectiveness of deploying the tools. The ideal balance is controversial and complex, and will depend on the policy and organisational context.[151] It may in some contexts involve more limited auditing rather than general public release.[152] For current purposes, it is important to note that the deployment of big data analytics in a non-transparent way may be harmful and run counter to the values of potential legal and police users as well as the broader community.

VI   CONCLUSION

> Technology is neither good nor bad; nor is it neutral.[153]

There is a risk in considering legal applications of big data that it is described as either inevitable or impossible. Part of the problem is the difficulty of understanding the techniques employed, the biases introduced in choosing a machine learning algorithm, the nature of the inferences drawn and the appropriateness of employing outcomes in decision-making. While these problems are common across empirical techniques, big data analytics is potentially more powerful, less transparent and hence more mythological than older techniques. The goal here is largely one of demystification – if we can understand the techniques, we can learn when and how to use them appropriately. While we cannot stop people doing statistics,[154] we can engage thoughtfully about the kinds of inferences that can and should be drawn and the influence such inferences ought to have on different kinds of decisions.

As is the case with a variety of tools, the means through which lawyers and law enforcers draw inferences and make decisions are not neutral. A move to treating legal decisions as data,[155] analysed by reference to statistical techniques,

---

150   Citron, above n 55.
151   Zarsky, above n 149.
152   Ibid.
153   Melvin Kranzberg, 'Technology and History: "Kranzberg's Laws"' (1986) 27 *Technology and Culture* 544, 545.
154   Bollier, above n 109.
155   Mayer-Schönberger and Cukier, above n 2.

rather than as precedents from which to construct doctrinal arguments, is significant. So is a shift to 'predictive policing' where deployment decisions are guided by statistical forecasting. The power of big data analytics and its potential effectiveness in identifying correlations may make a move in this direction attractive to some. However, this would need to overcome the traditional reluctance of lawyers and police to shift their customary frames of reasoning.

There are other factors relevant to the appropriateness of using big data analytics in legal and law enforcement decision-making. These are legality, accountability, and transparency. Such factors are relevant not only to the normative evaluation of these techniques, but also the likelihood that they will be accepted and taken up by public agencies, such as the judiciary and the police and ultimately the public. While there may be other factors in addition to these, it is these that are most likely to have a significant influence on the adoption and evaluation of computer tools in legal and law enforcement contexts.

It is possible to design and employ big data analytics in ways that enhance decision-making. It is also possible to use such tools in ways that are inappropriate or harmful. Telling the difference involves an understanding of how they work, what inferences can be drawn and how these can legitimately feed into decisions and actions. It also involves transparency in order to enhance accountability, ensure accuracy and guard against illegitimacy. We must remember that the existence of a tool does not make its use appropriate in every context. Both professional users and society more broadly should guard against the harms that might be caused by some applications of big data analytics, particularly when they influence the decisions of judges or police. The danger lies in any complacency or uncritical belief in the mythology of the 'truth, objectivity, and accuracy' of big data.[156]

---

156   boyd and Crawford, above n 38, 663.