Automatic justice?
Technology, Crime and Social Control

Amber Marks, Ben Bowling and Colman Keenan

In R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology, OUP, Forthcoming

Queen Mary University of London, School of Law
Legal Studies Research Paper No. 211/2015

TLI Think! Paper 01/2015

Editor: Peer Zumbansen, Director TLI / Managing Editor: Dayan Farias Picon

This paper can be downloaded without charge at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676154
Automatic justice?
Technology, Crime and Social Control

Amber Marks\(^1\), Ben Bowling\(^2\) and Colman Keenan\(^3\)

In R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology, OUP, Forthcoming

As science continues to change the social world, great transformations of factual inquiry lie ahead for all justice systems. These transformations could turn out to be as momentous as those that occurred in the twilight of the Middle Ages, when magical forms of proof retreated before the prototypes of our present evidentiary technology.


Abstract: This paper examines how forensic science and technology are reshaping crime investigation, prosecution and the administration of criminal justice. It illustrates the profound effect of new scientific techniques, data collection devices and mathematical analytical procedures on the traditional criminal justice system. These blur the boundary between the innocent person, the suspect, the accused and the convicted. They also blur the boundary between evidence collection, testing its veracity and probative value, the adjudication of guilt and punishment. The entire process is being automated and temporally and procedurally compressed. At the same time, the start and finish of the criminal justice process are now indefinite and indistinct as a result of the introduction of mass surveillance and the erosion against ‘double jeopardy’ protections caused by scientific advances that make it possible to revisit conclusions reached in the distant past. This, we argue, indicates a move towards a system of ‘automatic justice’ that is mediated by technology in ways that minimise human agency and undercuts the due process safeguards built into the traditional criminal justice model. The paper concludes that in order to re-balance the relationship between state and citizen in an automatic criminal justice system, we may need to accept the limitations of the existing criminal procedure framework and deploy privacy and data protection law which are now highly relevant to criminal justice.

Keywords: criminal justice; due process, surveillance, forensics, automation, technology, evidence, fair trial, data protection, privacy

---

\(^1\) Corresponding author. Lecturer in Criminal Law and Evidence, Queen Mary University of London. Email: a.marks@qmul.ac.uk Tel: +44(0) 20 7882 3964
\(^2\) Professor of Criminology and Criminal Justice, King’s College London
\(^3\) Dickson Poon Doctoral Scholar, King’s College London
Introduction

Technological and scientific developments have profound implications for the traditional paradigm of criminal justice and for the established relationship between state and citizen. Advances in the sophistication, range and ubiquity of forensic technology are part and parcel of ‘the creeping scientization of factual inquiry’ predicted nearly twenty years ago by Mirjan Damaška. (1997: 143) The goal of this paper is to examine the implications for the traditional model of criminal justice of new technologies in the investigation and prosecution of crime (Bowling, Marks and Murphy 2008). Our argument is that we are moving rapidly towards an increasingly automated justice system that undercuts the safeguards of the traditional criminal justice model. This system favours efficiency and effectiveness over traditional due process safeguards and is taking on a life of its own as it becomes increasingly mediated by certain types of technology that minimise human agency. This, we argue, is creating a system of ‘automatic justice’. In order to re-balance the relationship between state and citizen in such a system, we may need to accept the limitations of the existing criminal procedure framework and seek instead to unpick its core values for more effective deployment in the fields of privacy and data protection law, themselves rapidly evolving areas of law of increasing relevance to criminal justice.

The essay proceeds as follows: first, we provide an outline sketch of the traditional paradigm of criminal justice and its significance for the relationship between state and citizen; second we explain contemporary trends in criminal justice and explore how shifts in emphasis within the criminal justice system are facilitated and accelerated by advances in science and technology; third we examine how technological innovations affect the internal and external stability of the traditional criminal justice model and the implications of these changes in terms of its fundamental values. We illustrate how the pressure of technological innovations has made the external and internal boundaries of the criminal justice model more porous even while becoming increasingly securitized. In the absence of any clear boundary between the criminal justice system and the outside world, the privacy and liberty of all citizens is vulnerable to arbitrary state intrusion. Fourth and finally, we attempt to address the challenges identified by first exploring the possibility of applying criminal principles more broadly before briefly
turning to privacy and data protection law which may be capable of offering an alternative and additional architecture for upholding similar values to those enshrined within it (Damaška 1997: 147).

**The traditional criminal justice paradigm**

The criminal law has traditionally embodied the most coercive powers of the state for regulating the behaviour of citizens. Although the traditional model of criminal justice is conceptually elusive, certain normative values can be identified. Herbert Packer, in his classic text, describes what he calls the ‘due process’ model as containing an ‘obstacle course’ of procedural rules which safeguard against injustice while facilitating the pursuit of truth (Packer 1968: 163). In this sense we can speak of an ‘inner morality’ to criminal procedure (Duff and others 2007: 51); the criminal trial is its focal point, its main event in pursuit of legitimate dispute resolution between state and citizen. A core value of any liberal democracy is the principle of minimum state intrusion. Agents of the state are granted powers to coerce citizens, to intrude into their private lives and to deprive them of their liberty – as a means to pursue the ends of community safety and public order. The corollary to the granting of these intrusive and coercive powers to the state is that they must only be used when they are lawful, necessary and proportionate.

The criminal law consists of offences, the commission of which enables the state to punish a citizen by stigmatizing them, depriving them of their liberty or inflicting some other pains upon them. At the outset, and preceding the trial stage, criminal investigation necessitates reasonable, individualized and articulated suspicion as a prerequisite for investigation; where there is sufficient evidence against a suspect, that individual is charged with a specific criminal offence and the individual’s legal status becomes that of a defendant. The trial is central in this model: investigative powers are predicated on their ability to serve the trial process by producing evidence that can be examined and tested in a court of law, the factual determination and fairness of which will determine whether punishment is justified. A fair trial, then, is a pre-requisite of punishment and must take place within a reasonable time period. In the traditional model, the defendant either exits the criminal justice system at the conclusion of the process, or where punishment is justified, acquires the status of convict and is punished
by being retained within the system for a proportionate period of time.

The due process safeguards sewn into the traditional model have three overarching aims: (i) the minimization of state intrusion into the lives of citizens, (ii) the protection of human dignity, and (iii) upholding the legitimacy of state coercion and factual accuracy. Procedural propriety, concerned as it is with human dignity, is designed to ‘treat the accused as thinking, feeling, human subjects of official concern and respect, who are entitled to be given the opportunity to play an active part in procedures with a direct and possibly catastrophic impact on their welfare, rather than as objects of state control to be manipulated for the greater good (or some less worthy objective)’ (Roberts and Zuckerman 2010: 21). It is with this model in mind that we turn to modes of governance, trends and attendant technologies that are eroding and reshaping the criminal process.

**Prevailing Modes of Governance and Paradigm Shifts in Criminal Justice**

The criminal justice system has been subject to a great deal of change in the course of the last 40 years, often in complex and incoherent ways (O'Malley 1999). However, certain patterns and trends in criminal justice policy have tended to reflect prevailing modes of governance. A panoply of expressions have been proffered to capture the essence of the current mode of governance prevalent in Western liberal democracies: the hollowing out of the state (Rhodes 1994); the retreat of the state ( Strange 1996); governing at a distance (Rose and Miller 1992); a state that steers rather than rows (Osborne and Gaebler 1992); ‘the facilitating state, the state as partner and animator rather than provider and manager’ (Rose 2000: 327). All reflect an ideology, neoliberalism, in which the state seeks to enshrine the imperatives of economy, efficiency and effectiveness in its endeavours through the privatisation of many state functions while embedding business model ideals in others. This comes in the form of the new public managerialism, which injects a commercial ethos into public provision. The reification of the market and its mechanisms and the intense auditing of public bodies are central tenets of this mode of governance (Jones 1993). As such, the language and ethos of commerce have spread throughout the criminal justice system. Police forces are now required to ‘do more with less’ in the face of increasingly austere
budgetary constraints. The unwieldy edifice of the traditional ‘due process’ model of the criminal justice system, a system which prioritises fairness over efficiency, is deemed unfit for purpose. Increasingly, aided by advances in technology and science and in the interests of efficiency, individuals are investigated, judged and punished *en masse* and at a distance. Co-opting Rose and Miller’s ‘governing at a distance’, commentators now speak of a contemporary ‘punishment at a distance’ (Garland 2001: 179), a term which envisages a criminal justice system which regards individuals as little more than words and letters in a database.

We are witnessing a gradual movement away from the traditional, retrospective, individualized model of criminal justice, which prioritises a deliberated and personalized approach to pursuing justice and truth, towards a prospective, aggregated model, which involves a more ostensibly efficient, yet impersonal and distanced, approach. ‘Actuarial justice’ is based on a ‘risk management’ or ‘actuarial’ approach to the regulation of crime and the administration of justice (Feeley and Simon 1994). Feeley and Simon have characterised this as a movement away from concern for the individual offender, towards an emphasis on aggregates and ‘the development of more cost-effective forms of custody and control and (...) new technologies to identify and classify risk’ (Feeley and Simon 1992: 457). As described by Garland, ‘the individual is viewed not as a distinct, unique person, to be studied in depth and known by his or her peculiarities, but rather as a point plotted on an actuarial table’ (Garland 1997: 182). A central precept of actuarial justice, therefore, is that the system should be less concerned with traditional punishment based on downstream or after-the-fact goals such as retribution and rehabilitation. It should instead manage the risk presented by the dangerous and disorderly, using upstream or pre-emptive techniques of disruption, control and containment. The shift from retribution and rehabilitation towards prevention means that the state seeks to identify potential criminals before they commit offences. In light of such trends, Malcolm Feeley recently predicted the eventual emergence of a ‘unified actuarial ‘system’ that will completely transform the criminal process into an administrative system’ (Feeley 2006: 231).

Actuarial justice takes many and varied forms and is closely related to ‘intelligence-led policing’. This is a future-oriented mode of policing in which crime data are collected,
risks are assessed and policing strategies are formulated accordingly. (Maguire 2000) This is a departure from the reactive methods of policing prevalent up to the 1970s when '[t]he main organizational requirement was to arrive, do something, and leave as quickly as possible' (Sherman 2013: 378). Intelligence-led policing aims not merely to detect, investigate and prosecute offences, but to deter and disrupt the activities of those deemed likely to commit crime in the future. This form of policing has included the improper use of stop and search powers to deter and control certain types of behaviour, rather than to allay reasonable suspicions of criminal activity (Young 2008), heightened surveillance of 'high risk' residential areas (Joh 2014), the use of no-fly and other such watch list and blacklist regimes, citizenship-stripping and the use of newly created disposal alternatives to criminal prosecution in the form of civil preventive orders (such as anti-social behaviour orders (ASBOs) and Terrorism Prevention and Investigation Measures (TPIMs)) all of which result in often stigmatic and punitive repercussions for the individual involved, while obviating the procedural safeguards of the criminal trial. Such alternatives to criminalisation ‘define status, impose surveillance, and enforce obligations designed variously to control, restrict or exclude’ (Zedner 2010: 396).

Surveillance is a necessary correlative of risk-based actuarial criminal justice. (Lyon 2003: 8) While surveillance may be deployed in a wide-ranging variety of contexts and for similarly myriad purposes, in the context of crime control its purpose is to distil knowledge from uncertainty. Accordingly, it can be claimed that '[t]he yearning for security drives the insatiable quest for more and better knowledge of risk’ (Ericson and Haggerty 1997: 85). Michel Foucault’s panopticon (Foucault 1977) (as well as Orwell’s Big Brother (Orwell 1949)), conceived and abstracted in its broadest sense as unidirectional surveillance emanating from a monolithic, bureaucratic surveillance state has been a dominant and prevailing theoretical model of surveillance (Haggerty and Ericson 2000: 606). It is a model, however, that is indicative of the post-war state, cumbersome and lacking in dynamism and fluidity, which differs considerably from late modern surveillance, which traverses borders and institutions, both public and private, and expands in disparate and varied forms. At the turn of the century, Haggerty and Ericson, drawing on the influential work of Gilles Deleuze and Felix Guattari (1988), conceived of a 'surveillant assemblage', which expands upon, rather than departs from,
the panoptic surveillance model (Haggerty and Ericson 2000). This surveillant assemblage is rhizomatic in that surveillant capabilities develop and expand in a vast number of ways and in different contexts, combining to provide a complementary surveillant visage. One can also speak of different assemblages which combine and plug into each other (Haggerty and Ericson 2000: 608).

A further change in the criminal justice landscape that forms part of the backdrop to our discussion is the idea of ‘simple, speedy, summary justice’ (Home Office, Department of Constitutional Affairs and Attorney General’s Office 2006). Referred to as a ‘new form of administrative justice’ (Jackson 2008: 271), it overlaps with actuarial justice to the extent that both seek to divert potential offenders from the full rigour of criminal proceedings with alternative disposal proceedings. Simple, speedy, summary justice seeks to do this by increasing the range and uptake of pre-trial disposal procedures and its stated aim is the saving of expenditure: ‘What is changing is the scale of the number of cases proposed for diversion from the courts and the punitive steps that may be taken by prosecutors against those offenders who admit their guilt’ (Jackson 2008: 271). New forms of disposal include conditional cautions, reprimands, warnings for the young, fixed penalty notices, and a strengthening of administrative and financial incentives to admit offences and plead guilty early in the criminal justice process. Technology is shaped by these organisational goals, themselves moulded by prevailing modes of governance. In the case of the criminal process, incentives to ensure economy, efficiency and effectiveness embed administrative criminal processes that bypass fairness and legitimacy. The imperative of efficiency acts as an institutional incentive to adopt certain forms of technology and so ‘[n]ew technologies are routinely sold to criminal justice practitioners on their promised efficiency gains and cost savings’ (Haggerty 2004: 493).

‘New surveillance’, ‘New Forensics’ and ‘Big Data’

Three overlapping terms identify and capture what is novel and significant about the use of technology in the criminal justice field today: ‘new surveillance’ ‘second generation’ forensics’ and ‘big data’. Although each term could be used to describe applications of the same particular technologies – such as DNA profiling and CCTV –
each term connotes its own implications for the criminal justice context. ‘New surveillance’ involves ‘scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts’ (Marx 2005). The term is used to convey the relative intrusiveness of technology in extending the senses and rendering ‘visible much that was previously imperceptible’ (Kerr and McGill 2007: 393) and enabling law enforcement to undercut procedural safeguards by obtaining more information about citizens than would be available from a traditional search or questioning (Marx 2005). Erin Murphy (2007: 728-729) has written in detail on the characteristics of what she calls ‘second generation’ forensics, of which the following are pertinent to this essay:

(i) the highly specialized knowledge and expertise underlying them – which makes their workings less accessible and transparent to laypersons than traditional forensics;

(ii) the sophistication of the underlying science - which enables them to at least be portrayed as providing proof to a degree of scientific certainty and capable of providing conclusive proof of guilt. Whereas traditional forensics have generally played a supporting role (to eyewitness testimony and confession evidence, for example) second generation technologies are more frequently deployed as the sole piece of evidence; and

(iii) their dependence on databases and their ability to reveal a broad range of information (as opposed to being confined to the confirmation or denial of a specific question such as an identification) and their consequently deeper intrusion into privacy than traditional forensics.

‘Big data’ is generally accepted as an abbreviated expression for the application of artificial intelligence to the vast amount of digitized data now available and in this context much of the data will be obtained from ‘new surveillance’ and ‘second generation’ forensics. Such new methods of intelligence gathering are used to obtain more information than could be obtained from the traditional investigative techniques of questioning a suspect or subjecting them or their houses to a physical search, and
facilitate the automatic analysis of the data inputted. As pithily summarised by Elizabeth E. Joh, ‘the age of ‘big data’ has come to policing’ (2014: 35).

The combination of ubiquitous digital records and computer processing power has revolutionised profiling and social network analysis.1 Every time we make a phone call, send an email, browse the internet or walk down the high street, our actions may be monitored and recorded; the collection and processing of personal data has become pervasive and routine (House of Lords Select Committee on the Constitution 2009: 5). Dataveillance – ‘the monitoring of citizens on the basis of their online data’ (Van Dijck 2014: 205) – is a paradigm example of new surveillance. Advances in the use of mathematically based analytical tools to detect patterns in large sets of data have facilitated profiling (a method of data mining) (Bosco et al 2015: 7) whereby a set of characteristics of a particular class of person is inferred from past experience, and data holdings are then searched for individuals with a close fit to that set of characteristics’ (Clarke 1993: 405), in order to establish and identify patterns of suspicious behaviour. There is a general consensus amongst European Data Protection Authorities (DPAs) that the three principal characteristics of profiling are (1) that it is based on collection, storage and/or analysis of different kinds of data and (2) on automated processing and electronic means and (3) with an objective of prediction or analysis of personal aspects or personality and creation of a profile. Additionally a fourth key principle for some DPAs is that the profiling results in legal consequences for the data subject. (Bosco et al 2015:23) Data mining tools are used by the police to identify those who should be subjected to the growing proliferation of alternative control measures to the trial process outlined above. New surveillance coupled with risk based actuarial techniques and data mining technology seeks to make the best use of limited resources, and contributes to the increasing contemporary reliance on the intelligence-gathering, or absorbent, function of policing (Brodeur 1983: 513). Technology facilitates the transmission of information through space (communication) and through time (storage) (Hilbert 2012: 9). There is no physical barrier to storing all data – such as CCTV footage, facial images, etc. – indefinitely. Increasingly sophisticated means of recognition technologies and search tools will “one day make it possible to “Google spacetime”, to find the location of a specified individual on any particular time and date’ (The Royal Academy of Engineering 2007: 7).
Unlike traditional forensic science techniques such as ink fingerprinting and handwriting analysis, ‘second generation’ forensic technologies (Murphy 2007) such as digital fingerprinting and DNA typing draw on vast digital databases and do not require the police to first identify a suspect. Whereas first generation techniques were mainly used to confirm or deny suspicion, second generation techniques have heightened investigative capacities. The evolution of fingerprint technology illustrates this trajectory. Once limited to the identification of finger-print patterns in the search of individualized matches, the addition of mass spectrometry to fingerprint analysis has enabled detailed examination of these marks to reveal quite a lot about the personal and behavioural characteristics of the person who left the trace: their likely gender, the hygiene products they have used, the food ingested, whether or not they are a smoker, etc. As Alex Iszatt, writing in the Police Oracle, explained: ‘By analysing the constituent parts of the finger impression, we can profile the habits of the offender’ (Iszatt 2014). This development means that a print examination that may have failed to produce a suspect in the past can, if combined with data mining tools, produce a larger pool of potential suspects than traditional fingerprint identification. It also makes a database of the personal habits and lifestyle of the population a potentially useful resource for crime investigators, thereby providing further fodder for those seeking to legitimize the collection of personal data en masse and in the absence of prior suspicion. Fingerprint technology now enables digital fingerprints to be easily collected and immediately compared on the spot with others contained in a database.

‘Big data’ analysis, ‘new surveillance’ and ‘second generation’ forensic sciences lend themselves more easily to the new ‘actuarial model’ of criminal justice – based on computerized risk prediction and purportedly objective and conclusive results – than to individualized criminalization. The streamlined forensic reporting process recently introduced in English courts has the stated aim of cutting ‘costs and speed[ing] up the production of a forensic result: to undertake just enough forensic work to support a charge or secure an early guilty plea’ (Forensic Access 2014). New technologies play a key role in accelerating the trend towards ‘simple, speedy, summary justice’ by encouraging and facilitating diversion and discouraging costly challenges to prosecution evidence.
This decade a whole raft of miscarriages of justice has come to light in which wrongful convictions are attributed to mistaken expert opinion or the ineptitude of the traditional criminal justice model (populated as it is by non-scientific personnel) to correctly interpret technical and scientific evidence. Several high profile reports have been published in common law jurisdictions around the world seeking to address the problems. The perceived crisis in the traditional criminal justice model has deepened distrust of subjective knowledge and this has now extended from distrust in the layperson to distrust in expert opinion. The push is now to more and more purportedly objective data (Fenton 2013). Methods of decision making – understood to be objective, mathematical and scientific – are signalled as less biased than the ‘common sense’ exercised by human decision makers (Palmer 2012) and more adept at dealing with both the complexity and amount of scientific data:

[A]s the gulf widens between reality as perceived by our natural sensory apparatus and reality as revealed by prosthetic devices designed to discover the world beyond the reach of this apparatus, the importance of the human sense for factual inquiries has begun to decline (Damaška 1997: 143).

Forensic investigations are themselves increasingly automated (so-called ‘push-button forensics’) and this results in loss of understanding in the underlying concepts of the investigation amongst not only the recipients of the information (law enforcement agents, defendants and courts) but also the scientists actually conducting the forensic investigation. (James and Gladyshev 2013) Mobile handheld devices enable DNA and fingerprints to be taken from a suspect and analysed on the spot, providing an immediate –albeit potentially provisional– conclusion, and persuasive accusation. Such is the apparent superiority of automated methods to human decision-making that an increasing number of courts are aided by ‘safety assessment tools’ to reach decisions on bail applications and sentences (Dewan 2015; Leopold 2014). The reputed success of these tools calls into question the value of human decision-making with its attendant biases and lack of technical comprehension. Psychologist and academic, Mandeep Dhami doesn’t believe that the decision-makers in tomorrow’s courtroom will be human. Her research concludes that magistrates are ‘not as good as computers’ at reaching decisions and claims it is conceivable that magistrates ‘could be replaced by automated systems’ (Dhami and Ayton 2001: 163). Other researchers suggest that data
driven predictions and automated surveillance may actually reinforce prejudices and may even introduce a less readily transparent and ‘unintentional, embedded prejudice’ of their own (Macnish 2012: 151).

**Automatic criminal justice?**

Reliance on databases ‘that locate, identify, register, record, classify and validate or generate grounds for suspicion’ (Marx 2007: 47) results in ‘a broadening from the traditional targeting of a specific suspect, to categorical suspicion’ (Marx 2001). The ‘net-widening’ of those subjected to surveillance and control in the intelligence-led model of policing is facilitated and accelerated by the present day ubiquity of technologies of the so-called ‘new surveillance’. A common criticism of mass surveillance and data retention is that it makes ‘all citizens suspects’ and this is frequently deemed to be objectionable in and of itself.³ A system of crime control has emerged that operates in parallel to the traditional criminal justice system. The parallel system treats all citizens as suspicious and its surveillance is not predicated on individualised suspicion but is ubiquitous. It metes out heightened surveillance, control measures and punishments and places citizens on blacklists - sometimes on the basis of secret intelligence, without even communicating with the subject, in the absence of judicial oversight, and without providing any mechanism for redress (Sullivan and Hayes 2011).

Legislative changes have already made major inroads on the principle of double jeopardy in recent years in order to take advantage of scientific advances.⁴ A steady stream of scientific and technological advances will continue to increase the likelihood that new and compelling evidence that was unknown at the time of a defendant's acquittal will be discovered. Such developments blur the boundary between the absolved and the suspect and undermine the finality inherent in the traditional model. The parallel system challenges the external boundaries of the criminal justice system at both the exit and entry points; by-passing the procedural framework of the criminal justice system and the distinctions between citizen, suspect, defendant, convict and acquitted.
We are witnessing a simultaneous dissolution of the procedural infrastructure within the criminal justice system. The result of the actuarial trends described above, fortified by technological and scientific innovations, is that the traditional law enforcement regime has been ‘transformed from an investigatory into an accusatory and dispository regime’ (Jackson 2008: 272). Where wrongdoing is detected and proven, justice can be meted out instantly through the use of conditional cautions, fixed penalties for disorder, etc. rather like parking or speeding tickets. Aided by technology, the investigative and probative stages of the criminal justice process – which have traditionally been kept quite separate – are now merging into a single process that may be almost devoid of human judgement or engagement.

Automation is now routine in some spheres of policing and punishment. Take, for example, the investigation of motor vehicle licence and insurance investigation. In the UK, it has been estimated that the police seize about 500 vehicles per day where a police officer has reasonable grounds to believe that it is being driven without insurance (McGarry 2011: 220; Motor Insurers’ Bureau 2010). This intervention can arise from a routine police check, or a specialised ‘crackdown’ operation that are now used extensively by police forces across the United Kingdom. The process involves the use of Automatic Number Plate Recognition (ANPR) checks on vehicles that are then cross-checked against the Police National Computer (which is linked to the Motor Insurance Database (MID) and the Driver and Vehicle Licencing Agency (DVLA)) to determine whether there is a record of insurance (Kinsella and McGarry 2011). If there is not, a large sticker is placed on the windscreen stating that the vehicle has been ‘seized by the police driven without insurance’ and the vehicle is immediately loaded onto a car transporter and removed to the car pound. With a high degree of automation the offence is surveilled, investigated, detected and proven and the ‘offender’ punished, named and shamed. Connecting the dots, the near future of road policing is a system in which cameras connected to computers read motor vehicle licence plates automatically, recognise the faces of the driver and front seat passenger, detect the speed of the vehicle, connect these data to licensing and criminal databases, issue penalties and deploy officers to demobilise a vehicle and remove it from the road. In the context of the idea of the ‘internet of things’ – wherein mechanical devices speak directly to each other through computer networks – it is possible to imagine a world in which citizens are
investigated, evidence collected against them, a judgment of guilt reached and a penalty issued without the participation of a human being at any stage.

There are good reasons to anticipate that ‘automatic justice’ will soon be prominent in ordinary street policing. As discussed above, pre-emptive encounters inspired by technologies of risk are now permeating police activity at all levels (Hudson 2003). New devices – such as body-worn video cameras and those installed in vehicles – enable police officers to record encounters with the public in unprecedented ways. The evidence collected through these devices can be compelling and instantly reviewed by both police and suspect. The rolling out of tailored computer tablets will provide instant access to all police and other databases – both national and transnational – on all matters from criminal records of names, faces, fingerprints, DNA as well as criminal intelligence, licencing, insurance, welfare benefits and other personal information. The vision of the leadership of the police is to ‘use digital to connect the criminal justice system from the very first report of a crime through to a court appearance, an end-to-end service’ (Hogan-Howe 2015). The adoption of technology within law enforcement is perceived as ‘reaping the benefits of digital technology and smarter ways of working’ including an improvement in ‘quality of service’, productivity, efficiency and effectiveness (Hogan-Howe 2015). The Metropolitan Police Commissioner’s drive towards a ‘truly digital police force’ points in the direction of automatic justice.

**Some implications for Criminal Justice Values**

Twenty years ago Mirjan Damaška suggested that:

> [T]he Anglo-American procedural environment is poorly adapted to the use of scientific information (...) the scientization of proof is likely to exacerbate the presently minor frictions within traditional procedural arrangements. Their further deterioration should be considered likely on this ground alone (Damaška 1997: 147).

The developments outlined above strain the traditional concept of the trial as ‘a climactic event’ and beg the question of whether the public trial retains its status as the focal point in criminal procedure (Damaška 1997: 145). In facilitating and accelerating dramatic changes to the architecture of the criminal justice system, these new
technological developments raise urgent questions of procedural legitimacy. For example: how and at what stage will the reliability and accuracy of evidence be challenged? What is the fate of due process safeguards such as the presumption of innocence, the right to silence, the requirement of reasonable suspicion for the exercise of police powers, the right to a trial within a reasonable time, the principle of equality of arms and the right of confrontation? All are expressed in the procedural components of the traditional criminal justice model, but are rendered problematic in an automatic criminal justice system.

Unfortunately, as McGarry points out, automatic systems of policing – such as the investigation of uninsured driving – reverse the burden of proof, sometimes make errors, are experienced as heavy-handed, have few safeguards or means of correcting mistakes and have a significant impact on innocent individuals punished and shamed in this way (McGarry 2011). The challenges posed for due process by the trends and technologies outlined above are summarized by Wigan and Clarke in an article about the unintended consequences of ‘Big Data’:

> Decision making comes to be based on difficult-to-comprehend and low-quality data that is nonetheless treated as authoritative. Consequences include unclear accusations, unknown accusers, inversion of the onus of proof, and hence denial of due process. Further extension includes ex-ante discrimination and guilty prediction, and a prevailing climate of suspicion. Franz Kafka could paint the picture, but could not foresee the specifics of the enabling technology. (Wigan and Clarke 2013: 52)

Implicit in this paragraph and in the criticisms made by criminal law scholars of ‘speedy justice’ is the failure to engage with the suspect as an agent and the risk of persons being treated as guilty on the basis of inaccurate and unchallenged evidence (Jackson 2008).

Thus far, data mining and profiling are not reliably accurate in their behavioural predictions. As observed by Daniel Solove, given that most citizens are subjected to data mining techniques, even a very small false positive rate (1%) will result in a large number of innocent people being flagged as suspicious (Solove 2008: 353). As Valsamis Mitsilegas has pointed out, many will not have the possibility of knowing, let alone
contesting, such assessments (where they result in the flagging of suspicious behavior for example) (Mitsilegas 2014). Even where they do, the assumptions that algorithms contain may not only be incorrect, but will also be difficult to spot because they are ‘hidden in the architecture of computer code’ (Solove 2008: 358). Legal practitioners have expressed concern about the ‘aura of infallibility’ that surrounds mathematically generated information, deterring attempts to understand the process by which results are reached and inhibiting challenges to their accuracy (Eckes 2009: 31).

High levels of accuracy and certainty are required for criminal convictions (the case must be proven beyond reasonable doubt) on account of the cost of error both to the state (in terms of legitimacy and financial cost) and to the individual (in terms of stigma, financial loss or deprivation of liberty) (Roberts and Zuckerman 2010: 17). The issue that needs to be considered in relation to profiling of suspicious behavior is working out the cost of error to both the state and the individual. Such evaluations should consider not only the cost of being singled out for extra investigation or for inclusion on a blacklist and the service denials entailed (Ramsey 2014), but also the more abstract implications for rights such as the freedom of association and the right to privacy, given that much of the data used in generating the profile will come from the lawful exercise of such rights (Solove 2008: 358).

Law enforcement agents may not always appreciate the potential for error in new technologies and defer their judgment and decision-making to technology. The relevance (Marks 2013) and reliability (Law Commission 2011) of scientific evidence are often incorrectly evaluated by legal systems. Concerns have been expressed about the so-called ‘CSI effect’ in relation to misplaced police, judicial and jury deference to forensic science. Scholars have been equally concerned with vulnerability of legitimacy of the verdict if courts are seen to defer to expertise: ‘The fear is spreading that courts are covertly delegating decision-making powers to an outsider [expert] without political legitimacy. Is the court’s nominal servant becoming its hidden master?’ (Damaška 1997: 151) According to Roberts and Zuckerman, if this fear regarding deference to science and technology turns out to be well-grounded, it would amount to a radical realignment of criminal trial procedure (Roberts and Zuckerman 2010: 489). Total reliance upon science represents ‘an abdication of responsibility by law’ (Alldridge 2000: 144).
It is clear that the criminal justice system will command more support from the public if its procedures, techniques and outcomes are easily and widely comprehensible. This is undermined by a system of increasingly automatic justice that relies heavily on scientific procedures, mathematical calculations and technical devices. The prospect of uniform data collection and permanent data retention has several implications for the criminal justice model. The criminal justice system is designed to not broadcast information about minor offenses, and in many countries criminal records systems actively omit old offenses when performing criminal records checks. The system thus favors forgiveness and rehabilitation, rather than permanently labeling people as criminals. Indiscriminate data retention conflicts with such constructive aims (Wigan and Clarke 2013: 51).

**Meeting the Challenge**

The challenge is how to ensure that ‘automatic justice’ retains the characteristics of ‘justice’ and is in accordance with fair trial rights. On the one hand there are the challenges to criminal justice values within the traditional model, and on the other there are those posed by the emergence of the parallel model of crime control that may entail greater state intrusion and coercion than that of the traditional criminal law. Predictive mass surveillance (as opposed to targeted reactive surveillance) is largely unregulated by criminal justice procedures and yet it is arguably more intrusive on privacy rights on account of its endurance where data is stored indefinitely. The legality of much of it is also far from clear. Judgments of the European Court of Human Rights and the European Court of Justice have made clear that the mere retention of personal data, regardless of what is consequently done with it, amounts to intrusion into privacy (S and Marper v United Kingdom (2009); para 67). The court has also decided that blacklisting regimes must comply with fundamental rights including the right to a defence as guaranteed by Article 6 of the European Convention on Human Rights. (Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission [2008]) Mirelle Hildebrandt has described the fundamental principles of criminal procedure as historical artefacts that should not be taken for granted. They should instead be acknowledged as the foundations upon which any liberal democracy – including one operated by sophisticated technology – must rest (Hildebrandt 2008). We perceive
three means of addressing the challenges posed by automatic justice to the fundamental values traditionally enshrined in criminal procedure: (i) extending the procedural requirements outside of the traditional criminal justice model; (ii) incorporating criminal justice values within the rapidly evolving and heavily contested field of data protection law; (iii) incorporating lessons learned in data protection law within the criminal justice system.

*Extending the Scope of the Criminal Justice Model*

In light of the range of alternative disposal measures and the wide reach of new technologies it is arguable that the threat of criminal investigation, prosecution and conviction no longer represents the most coercive arm of the state and that the citizen/suspect and suspect/convict distinctions no longer hold water. As has been persuasively argued by Liz Campbell, ‘this may imply that some of the traditional protections that relate to the criminal trial, strictly speaking, are valuable or necessary in a wider context’ (Campbell 2013: 689). Because surveillant, investigative, probative and punitive powers have migrated out of the criminal justice system and are now more widely diffused throughout society, there is a need for the due process protections with which they are associated to follow suit. Several scholars and courts have recognised the importance of extending judicial oversight and due process safeguards to the administration of potentially punitive measures such as watch-lists (Ramsey 2014).

The ubiquity of new surveillance raises the question of what it means to be a suspect. Some scholars have gone so far as to claim ‘the concept of suspect is now thoroughly transformed, for we are no longer able to confine it to its juridical sense’ (Bauman and others 2014: 138). Liz Campbell argues that we should recapture the concept of suspect within its juridical sense by widening it to include an ‘interim categorisation of suspicion’ (Campbell 2010: 898) for those treated by the state in a manner that suggests they are not ‘wholly innocent’ (*S and Marper v United Kingdom* (2009): 89). This interim category is reserved for retaining information on a mass scale of certain targeted categories of people, premised on the perceived risk they pose. A status of ‘proto-suspect’ could entail a measure of suspect’s rights. As well entailing an expansive interpretation of the presumption of innocence this reconceptualization of the suspect
suggests the core of being a suspect is to be treated differently to others. There is a
danger of conflating the concept of suspect with the concept of convict here however,
which itself reflects a tension in the application of the presumption of innocence and the
extent to which it should apply to pre-trial measures as well as to the trial, let alone to
the more recent debate over extending it to alternative disposal measures.

The apparent similarities between the treatment of convicts and the treatment of
persons who are not even suspects gained ground for the right to privacy in *S and
Marper v United Kingdom* (2009) by curtailing the retention of the DNA of persons
other than those convicted of criminal offences. But the logical conclusion of applying
the protection of the presumption of innocence only where persons are treated
differently to those who are ‘wholly innocent’ fails to protect privacy in the long term if
citizens are all subject to different forms of mass surveillance and data retention. In
addition to further exploring the values underpinning the presumption of innocence –
particularly in relation to its potential application to regulatory measures that look like
criminal punishments (punishment as ‘communicative act’), it may be useful to think
about what negative consequences, other than stigmatization, could be said to be at the
core of being a suspect.6 We might look at the values underpinning the principle of
double jeopardy for further guidance.7 An important value said to underpin the
principle of double jeopardy is finality. There is value to the suspect and to society as a
whole in accepting that a contested issue (i.e. the criminality of the suspect) has been
resolved (Ashworth and Redmayne 2010: 399). In the absence of resolution one
remains a suspect under permanent threat of state coercion into an indeterminate
future. There are undoubtedly other important aspects to the status of suspect and this
could prove useful terrain for those seeking to address the perceived injustices of mass
surveillance.

*Incorporating developments in privacy and data protection law within the criminal
justice system*

Alldridge and Brants (2001: 5) argue that ‘as proactive policing increases in
importance, consequently, so should attention be devoted to the claims of privacy in
criminal procedure’.8 Evidence scholars have highlighted the threat posed to privacy by
disproportionate intrusions in the form of the combined relaxation of the rules on the admissibility of bad character evidence, broad definition of such, and the wealth of personal data now accessible online. As Roberts and Zuckerman (2010: 599) put it, ‘empowering the authorities to require the accused to answer at large for his entire existence and moral character would not be compatible with liberal conceptions of limited government.’ Greater attention needs to be paid to protecting a defendant’s right to privacy within the traditional criminal justice model on account of the reach of ‘new surveillance’ and ‘second generation’ forensics.

We focus on the right to privacy on the basis that ‘privacy is to proactive policing what due process is to reactive policing’ (Alldridge and Brants 2001: 21). The raison d’être of laws on police searches is to protect a citizen’s personal space from arbitrary interference but new technologies bypass such safeguards by obviating the need for traditional stop and searches. (R v Dyment [1988]) New surveillance practices and technologies - such as thermal imaging and millimetre waves can investigate a person’s belongings without making physical contact and without the subject even being aware that they are being ‘searched’. The use of meta-data from personal communications ‘may make it possible to create a both faithful and exhaustive map of a large portion of a person’s conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity’ (Digital Rights Ireland Ltd v Minister for Communication [2014], Opinion of AG Villalón, para 74).

Effective metrics for balancing the effectiveness and utility of new technological means of investigation and surveillance against the intrusiveness of the privacy invasion are in their infancy. The concept of privacy, therefore, is in urgent need of clarification in order to ensure that the laws designed to protect it are applied effectively and enabled to keep pace with technological innovation (Metcalfe 2011: 99; The Royal Academy of Engineering 2007). The challenge facing scholars is to clarify the concept of privacy in this context. An initial task is to develop a list of indicators of intrusiveness. Several attempts have been made to gauge the relative intrusiveness of various potential intrusions on privacy by conducting surveys of public attitudes. Another approach would be to draw on the criminal law on battery. This draws on ‘background social norms’ to delineate the boundaries of personal space and determine the extent of any
intrusion (Florida v Jardines (2013): 7). The offence of battery does not include 'everyday touching' or 'generally acceptable standards of conduct', for example bumping into someone on a crowded tube train or tapping someone on the shoulder to inform them that they have dropped something (Collins v Wilcock [1984]). In a new world of digital communication in which so much of our personal lives are now conducted on digital formats (Roux and Falgoust 2013), these background norms are still in embryonic form.

There is an ‘obvious link’ between the right to privacy and the law on data protection and this relationship as well as the potential for safeguarding privacy in data protection law has been examined in detail elsewhere (Stoeva, 2015). Intelligence and law enforcement officials were largely untouched by early data protection regulations (Data Protection Directive 1995, DPD) on account of broad exemptions for activities in pursuit of crime prevention and security (Bignami, 2007). Nonetheless, there are clear parallels to be drawn between concerns expressed about police and court deference to science and technology in the criminal justice system and those exercising the drafters of Article 15(1) of the EC Data Protection Directive on the protection of individuals with regard to the processing of personal data. Article 15 is the only provision of the DPD to grapple directly with automated profiling and its drafters expressed concern that the ‘increasing automation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans’ (Bygrave 2001: 18).

A similar discomfort can be detected in judicial reluctance to convict defendants on the basis of statistical evidence alone, a prospect described as abhorrent by several evidence scholars on account of it being 'the wrong kind of evidence' (Duff 1998: 156). There is further resonance between the concerns underlying Article 15 and those motivating the protections enshrined in criminal procedure, which can be encapsulated in the concern to preserve human dignity with the principle of humane (or even human!) treatment. Article 15 was ‘designed to protect the interest of the data subject in participating in the making of decisions which are of importance to them’ (Commission of the European Communities 1990: 29). The rules of criminal procedure in the traditional criminal justice model share this objective. Recent decisions on
hearsay in the European Court of Justice have reinvigorated debates on the meaning and importance of the ‘right to confrontation’ (O'Brian Jr 2011; Redmayne 2012). How well does this right - the right to confront one’s accuser - sit with the prospect of the ‘automated accuser’? (Wigan and Clarke 2013: 52)

The European data protection framework is presently under revision and the proposed new Data Protection Regulation is expected to enter into force in 2015. Debates about the extent to which the proposed new Regulation succeeds in grappling with the ‘computational turn of the 21st century’ and the ‘large-scale, complex, and multi-purpose forms of matching and mining zettabytes of data’ implied, is a hot topic of debate in data protection and of clear relevance to an increasingly automated criminal justice system (Koops 2013: 215). Additions to the aforementioned Article 15 (Article 20 in the proposed new Regulation) have been described as providing a potentially ‘revolutionary’ step forwards in levelling the playing-field in profiling practices by obliging data controllers to provide information as to the existence of processing for an automated decision and about the envisaged effects on the data subject (Koops 2013: 200). However, the proposed new Regulation has been criticised for confining its focus to ex-ante process transparency and for failing to extend its reach to ex-post outcome/event/decision transparency. (Koops 2013: 200) Greater decision transparency is advocated for ‘in the form of understanding which data and which weight factors were responsible for the outcome’ on the basis that it is this, as opposed to the subject’s awareness of their participation in the provision of data, that would enable a decision based upon its analysis to be effectively challenged or revised (Koops 2013: 213). According to art. 12(a) DPD, each data subject has the right to obtain from the controller ‘knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)’. That is, ‘a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.’ (articles 12(a) and 15(1) DPD). This element of data-protection legislation has been described as particularly suited to enhance outcome/decision transparency, however it has been criticised for being confined in its application to decisions that are fully automated and the fact that it is a user-triggered
access right as opposed to a provider-focused information duty (Koops 2013: 211).

Although the European Data Protection Regulation will not apply to law enforcement (the same exemptions apply to the prevention of crime as in the DPD it is proposed to replace), debates about decisional transparency in data protection should have greater resonance in the criminal justice system. Indeed, consideration of European data protection debates has led some scholars to question the reasons for 'the police and justice sector being handled differently and separately from other sectors' in the proposed Data Protection Reform Package (Cannataci, 2013). A directive was introduced in 2008\textsuperscript{12} for application to law enforcement and the proposed Data Protection Reform Package proposes to replace this with a new Directive (the present directive has been criticised for only applying to exchanges of personal data between Member States and not the processing of police data within each member state) rather than incorporating law enforcement within the European Data Protection Directive. Both the 2008 Directive and the latest draft for its proposed replacement include articles prohibiting decisions which have an adverse legal effect for the data subject or significantly affect them to be based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests. Neither directive includes an equivalent to article 12 of the DPD, however, and there is no reference to the logic of automated processing in either the present or the proposed directives of application to law enforcement. Recent changes to the Criminal Procedure Rules on expert evidence in England and Wales (along the lines recommended by the Law Commission) seek to ensure that wherever expert opinion is admitted at trial, the basis for that opinion is laid bare in a manner comprehensible to lay persons. Where alternative disposal methods are invoked decision transparency is obfuscated and as discussed above, particularly where the inferences drawn are based on complex algorithms, even those exercising the decision may be ignorant of the details of the inferential process used. Should citizens have a right to be informed of the logic behind decisions to flag their vehicles as suspicious? (Koops, 2013) Should this be the case wherever the decision is based on human judgment, semi-automated or fully automated processes?
Incorporating criminal justice values within the rapidly evolving and heavily contested field of data protection law

There is widespread misunderstanding and ambiguity surrounding the extent to which data protection regulations apply to law enforcement (O’Floinn 2013) but data protection bodies are increasingly drawing on the ‘due process’ values developed over many years in the theory and practice of the criminal law. The UK Information Commissioner recently acknowledged that the principle of fair and lawful processing of data is engaged when a public statement by the police undermines the presumption of innocence. In a statement issued by the ICO, a spokesperson explained:

The ICO spoke to Staffordshire Police following its #DrinkDriversNamedonTwitter campaign. Our concern was that naming people who have only been charged alongside the label ‘drink driver’ strongly implies a presumption of guilt for the offence, which we felt wouldn’t fit with the Data Protection Act’s fair and lawful processing principle’ (Baines 2014).

Such a development in the application of data protection principles could go some way towards addressing concerns expressed by Campbell about the procedural impediments to expanding the presumption of innocence to state practices outside of the traditional model such as inclusion on ‘watch lists’, and publication of civil preventative orders (Campbell 2013). Although in the case dealt with by the Information Commissioner, the persons named had been charged and were awaiting trial, the fact that the spirit of the presumption of innocence could be incorporated within the fair and lawful processing principle is a promising development.¹³

Conclusion

Historically, the parameters of government control over the citizen have been most clearly articulated in the rules of criminal procedure and evidence. This is largely on account of the criminal law having traditionally provided the state with its most coercive and intrusive powers and mechanisms with which to carry out surveillance, control and punishment. (Bowling, Marks and Murphy 2008) Recent technological innovations have exacerbated tensions in the traditional model of criminal justice to the
point that its internal and external boundaries are on the brink of collapse. New scientific techniques, data collection devices and mathematical analytical procedures are having a profound effect on the administration of criminal justice. They are blurring the boundary between the innocent person who should be able to expect freedom from state intrusion and coercion and the ‘reasonably suspected’ person for whom some rights may justifiably be curtailed. These same technologies are also blurring the boundary between the accused and the convicted. The established process that distinguishes the collection of evidence, the testing of its veracity and probative value and the adjudication of guilt are being automated and temporally and procedurally compressed. At the same time, the start and finish of the criminal justice process are now indefinite and indistinct as a result of the introduction of mass surveillance and the erosion of ‘double jeopardy’ protections caused by scientific advances that make it possible to revisit conclusions reached in the distant past. In our opinion, this drift is endangering the privacy and freedom of all citizens and most perniciously that of the ‘usual suspects’. There may be scope for protection in expanding the application of criminal justice safeguards to everyone. However, it may be that the speed and depth of the technological changes occurring in this area are so great that the traditional criminal justice model – with such precepts as the presumption of innocence, the separation between the collection of evidence by the police and the testing of that evidence by a court of law and so on – is no longer fit for the purpose of explaining criminal justice practice or constraining state power. Our deepest concern is the emergence of a potentially unfettered move towards a technologically driven process of ‘automatic criminal justice’. It may be that a stronger right to privacy and enhanced data protection rights could prove a more solid foundation for building a model that will protect fundamental human rights and civil liberties in the long term. We think that in an increasingly digital world, further exposition of traditional criminal justice values is required along with a detailed examination of how these values can be combined with data protection developments to provide proper safeguards in the new technologically driven world of criminal justice.
Reference List


Cannataci JA, 'Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector' (2013) 4(2) European Journal of Law and Technology


Damaška MR, Evidence Law Adrift (Yale University Press 1997)

Deleuze G and Guattari F, A Thousand Plateaus: Capitalism and Schizophrenia (Bloomsbury Publishing 1988)


Eckes C, EU Counter-Terrorist Policies and Fundamental Rights: the Case of Individual Sanctions (Oxford University Press 2009)

Ericson RV and Haggerty KD, Policing the Risk Society (Oxford University Press 1997)


Fenton N, 'Effective Bayesian Modelling with Knowledge before Data' (2013) ERC Advanced Grant 2013 Research proposal [Part B1]

Foucault M, Discipline and Punish: The Birth of the Prison (Vintage 1977)


——, The Culture of Control: Crime and Social Order in Contemporary Society (Oxford University Press 2001)


Hilbert M, 'How much Information is there in the “Information Society”?' (2012) 9 Significance 8-12

Hildebrandt M, 'Ambient Intelligence, Criminal Liability and Democracy' (2008) 2 Criminal Law and Philosophy 163-180


Joh EE, 'Policing by Numbers: Big Data and the Fourth Amendment' (2014) 89 Washington Law Reform 35-68
Koops B-J, 'On decision transparency, or how to enhance data protection after the computational turn' in Hildebrandt M and Vrie Kd (eds), Privacy, Due Process and the Computational Turn (Routledge 2013)
Law Commission, Expert Evidence in Criminal Proceedings in England and Wales (Law Com No 325, 2011)
———, 'Surveillance and Society' in Ritzer G (ed), Encyclopedia of Social Theory (Sage Publications 2005)
McGarry J, 'Named, Shamed, and Defamed by the Police' (2011) 5 Policing 219-227
Metcalfe E, Freedom from Suspicion: Surveillance Reform for a Digital Age: A Justice Report (Justice 2011)


O'Floinn M, 'It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe' (2013) 29 Computer Law and Security Review 610-615

O'Malley P, 'Volatile and Contradictory Punishment' (1999) 3 Theoretical Criminology 175-196

Orwell G, 1984 (Secker and Warburg 1949)

Osborne D and Gaebler T, Reinventing Government: How the Entrepreneurial Spirit is Transforming Government (Addison-Wesley 1992)

Packer H, The Limits of the Criminal Sanction (Stanford University Press 1968)


Redmayne M, 'Confronting Confrontation' in Roberts P and Hunter J (eds), Criminal Evidence and Human Rights (Hart Publishing 2012)


Roberts P and Zuckerman A, Criminal Evidence (2nd edn, OUP 2010)


Roux B and Falgoust M, 'Information Ethics in the Context of Smart Devices' (2013) 15 Ethics and Information Technology 183-194


The Royal Academy of Engineering, Dilemmas of Privacy and Surveillance: Challenges of Technological Change (The Royal Academy of Engineering 2007)


Cases

Collins v Wilcock [1984] 1 WLR 1172

Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communication [2014], Opinion of AG Villalón

Florida v Jardines 569 U.S. (2013)

R v Dyment [1988] 2 SCR. 417

S and Marper v United Kingdom (2009) 48 EHRR. 50

**Legislation**

Criminal Justice Act 2003

Data Protection Act 1998

Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data


See for example quotation from Carole McCartney in ‘Universal DNA database would make us all suspects’ New Scientist 19 September 2007.


We have borrowed this terminology from Mirelle Hildebrandt’s discussion of how to preserve the achievements of constitutional democracy in a world of ambient intelligence, see p.167 ‘Ambient Intelligence, Criminal Liability and Democracy’ Crim Law and Philos (2008) 2:163.

For a detailed unpacking of the presumption of innocence including an exploration of the basic notion of ‘innocence’ as well as the historical role of the presumption in shielding the accused from the hardships of the criminal process see C-F. Stuckenbring ‘Who is Presumed Innocent of What by Whom’ Crim Law and Philos (2014) 8: 301-316.


Article 15 grants the right to every person not to be subject to a decision which produces legal effects concerning them or significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to them.
COUNCIL FRAMEWORK DECISION 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.