The Fourth Workshop on the Social Implications of National Security

The Social Implications of Covert Policing

7 April 2009

National Europe Centre, ANU, 1 Liversidge Street, Canberra

Editors: Simon Bronitt, Clive Harfield and Katina Michael

Editors: Bronitt, S., Harfield, C. and Michael, K.

Publication Title: The Social Implications of Covert Policing (Workshop on the Social Implications of National Security, 2009)

Series: Centre of Excellence in Policing and Security (CEPS) / Research Network for a Secure Australia (RNSA)

Publisher: University of Wollongong Press, the Centre for Transnational Crime Prevention, Faculty of Law

Publication Year: 2010

Contact Details: Tel 02 4221 3937, Fax 02 4221 4045, University of Wollongong NSW 2522

Conference Websites:
http://ceps.edu.au
http://www.secureaustralia.org
http://www.anu.edu.au/NEC/conferences_workshops/2009_CrossingBorders/Covert-Program.pdf
http://www.uow.edu.au/~katina/rnsa09.htm
http://www.ceps.edu.au/?q=events/Workshop-Social-Implications-Covert-Policing-Workshop

Format: Book (hardcopy $50 AUD; softcopy free from http://ro.uow.edu.au/kmichael)

Cover and text layout: Anthony Petre and Roba Abbas

Front Cover Image: the artwork 'big bother' (Cambridge 210806) was created by Mr Josh Wodak from the exhibition The *Rights to Which we are All Entitled*. Commissioned solo photography exhibition at National Europe Centre, ANU. December 13, 2008 – February 20, 2009.

ISBN: 978-1-74128-193-4 (print)
ISBN: 978-1-74128-194-1 (pdf)

This event is organised by the ARC Centre of Excellence in Policing and Security (CEPS) with some support from the Research Network for a Secure Australia (RNSA).

CEPS was established by the ARC in 2007 to boost policing and security research capacity in Australia amid the growing complexity and internationalisation of transnational crime in the post 9/11 environment.

CEPS is a complex research enterprise consisting of multiple collaborating researchers, and university and partner organisations. CEPS is administered by Griffith University in Brisbane and operates across four University Nodes. The university nodes include Griffith University, the Australian National University, The University of Queensland and Charles Sturt University.

CEPS Director:	Prof Simon Bronitt, CEPS Executive, Griffith University
CEPS Deputy Director:	Prof Peter Grabosky, Professor in the Research School of Pacific and Asian Studies at the Australian National University

RNSA is a multi-disciplinary collaboration established to strengthen Australia's research capacity for protecting critical infrastructure (CIP) from natural or human caused disasters including terrorist acts. The RNSA facilitates a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to mitigate emerging safety and security issues relating to critical infrastructure. World-leaders with extensive national and international linkages in relevant scientific, engineering and technological research will lead this collaboration.

RNSA Convenor:	Prof Priyan Mendis, Head of the Advanced Protective Technology for Engineering Structures Group at the University of Melbourne

Both CEPS and the RNSA organise various activities to foster research collaboration and nurture young investigators.

Foreword

Police agencies have been accused of suffering from an acute form of technophilia.[1] Rather than representing some dreadful disorder, this assessment reflects the strong imperative, both in police agencies and the wider community, that police must have access to the latest technologies of surveillance and crime detection.

The last decade has witnessed the proliferation of low-cost surveillance technologies, some developed specifically for law enforcement purposes. Technology once the preserve of the military or secret intelligence agencies is now within the reach of ordinary general duties police officers. The new generation of police recruits is highly adept at using new technologies. Indeed, there is evidence that some police carry their own personal audio and video recorders and use them to provide independent evidence of 'difficult' interactions with citizens. Indeed, some jurisdictions are now trialling the use of miniaturised wearable point of view (POV) cameras attached to police officer's uniforms.

It is clear that advances in Information and Communication Technologies (ICT) enable the covert surveillance of people, property and spaces, both public and private. In many jurisdictions, police now require warrants or some form of independent authorisation to track and monitor suspects or places using surveillance devices. But the old adage that technology outstrips the law's capacity to regulate still remains true: each round of technological innovation poses a new range of social and legal challenges. Surveillance technologies generate concern about unjustified invasions of privacy and property; but there are also new threats to the fair trial, since the use of these technologies potentially circumvent the legal safeguards (such as the privilege against self incrimination) that may otherwise apply.

The modern trend seems to favour the statutory regulation of police powers. The expanded powers of telecommunications interception over the past three decades (which now extends to access to stored communications) are a case in point. However in many jurisdictions that the laws governing covert policing are patchy and in some areas completely unregulated. In the heightened climate of national security, human rights considerations tend to be sidelined, with law enforcement agencies gaining wide access to personal data such as mobile phone and Internet Service Provider (ISP) records. To preserve public confidence in the system and legitimacy, there is a need to maintain high levels of compliance with domestic legal requirements and international human rights standards.

It is important that police and policy-makers not lose sight that the use of new technology is not an end in itself, but rather simply a means to an end: namely, the prevention, detection and prosecution of crime. Infiltration of organised cross border criminal networks undoubtedly requires more sophisticated evidence-gathering

1 Benoit Dupoint, "Police technophilia: Toys for the boys in blue", *Legaldate*; July 2002, Vol. 14, Issue 3, p. 4.

techniques. These techniques include proactive policing operations using 'reverse stings' or controlled deliveries, as well as use of covert interviewing by undercover police and informers. In an era of increased international police cooperation across borders, there is a pressing need to explore how new law enforcement technologies and techniques may be more effectively coordinated and managed, while at the same time maintaining public confidence. The picture is not however universally bleak as new technology brings the potential for enhanced systems of regulation with a higher degree of transparency and accountability than previously possible, as exemplified by the introduction of audio-visual recording of police interviews and CCTV in police stations more generally.

This volume is based on a selection of papers presented at a workshop held in April 2009 at the ANU in Canberra. The workshop canvassed a wide range of topics addressing the application of covert surveillance techniques in policing and their social implications. Participants were drawn from a range of professions and disciplines including policing and intelligence studies; criminology and criminal justice; Information and Communication Technologies (ICT); law, ethics, human rights and public policy. As a group, participants recognised the need to equip law enforcement with the right tools for the job, though the corollary was the consensus that new and emerging technologies need to be regulated effectively. The discussion also underscored the importance of not limiting debate about reform to technical or technological perspectives. Wide normative concerns (drawn from a legal, human rights, public policy or ethical perspectives) must also be addressed.

The workshop and the resulting publication is an initiative supported by the Australian Research Council Centre for Excellence in Policing and Security (CEPS) and Research Network for a Secure Australia (RNSA), and the editors acknowledge their generous support for the workshop and publication.

Simon Bronitt, Griffith University
Clive Harfield, University of Wollongong
Katina Michael, University of Wollongong
December 2010

Workshop Convenors

Simon Bronitt, Griffith University
Katina Michael, University of Wollongong

Organising Committee

Simon Bronitt, Griffith University
Saskia Hufnagel, Canberra University
Priyan Mendis, University of Melbourne
Katina Michael, University of Wollongong

Reviewers

The editors would like to thank the following reviewers for their assistance in maintaining the quality of papers.

Ms Roba Abbas	Research Assistant, School of Information Systems and Technology, University of Wollongong
Dr Anas Aloudat	Research Assistant, School of Information Systems and Technology, University of Wollongong
Professor Simon Bronitt	Executive Director of Centre of Excellence in Policing and Security, Griffith University
Associate Professor Clive Harfield	Centre for Transnational Crime Prevention, University of Wollongong
Professor Allyson MacVean	Director of the John Grieve Centre, London Metropolitan University, UK
Mr Peter Mahy	Partner (Civil Liberties and Human Rights team) at Howells LLP, UK; Legal Aid Lawyer of the Year 2010
Associate Professor Katina Michael	School of Information Systems and Technology, University of Wollongong
Honorary Senior Fellow MG Michael	School of Information Systems and Technology, University of Wollongong
Associate Professor Nick O'Brien	Australian Graduate School of Policing, Charles Sturt University

Table of Contents

Peer reviewed papers are identified with an asterisk.

1

Regulating covert policing methods: From reactive to proactive models of admissibility

Simon Bronitt
Griffith University

Abstract

In this paper I will explore (a) how the courts, through their judicial discretion to exclude evidence and procedural rules, regulate the admission of evidence, and (b) the impact (if any) that court rulings have on investigative practices. Focusing on a range of examples from the field of covert investigation (including controlled operations and covert interviewing), this paper will explore the effectiveness of this model of judicial review. The paper explores whether, in lieu of post hoc judicial review, there are other regulatory models that could be employed proactively to determine the admissibility of evidence in cases where the legality and ethics of investigative methods are contestable.

Keywords: covert policing, regulation, judicial review, admissibility of evidence

Introduction

The current regulatory framework in Australia governing covert evidence-gathering methods is a patchwork of federal, state and territory laws. In the last decade a wide range of covert investigation methods, including covert interviewing and scenario testing, have been embraced with enthusiasm by law enforcement agencies around the globe.[1] These new techniques have supplemented existing powers relating to use telecommunications interception (wiretapping), controlled operations, and electronic surveillance devices.[2] But there are problems with this governance framework.

First, the Australian framework, being based on a federal constitutional system, does not provide a national (or indeed a uniform) scheme of regulation. Second, regulation and reform tends to be device-specific with the inevitable consequence that new and emerging technologies and practices outstrip the law's capacity to regulate. The result is that some investigative practice unregulated, or more precisely are unregulated until the courts and common law turn attention to the legality of these techniques in the context of litigation.

The current system, with a heavy reliance on *post-hoc* scrutiny of evidence on the grounds of unfairness, illegality or impropriety is a poor regulatory system for covert policing for a number of reasons. Foremost, our current model is *reactive*: it tends to generate the legal norms after the event, reacting to defence challenges in the context of litigation. It fits well with Jeremy Bentham's jibe about judge-made common law as being "Dog Law" for it condemned individuals after the event, in the way that an owner punishes his dog. The dog only learns after the punishment that what it has done is wrong.[3] Appeal court judgments, with their multiple speeches and rambling narrative style, are particularly poor mechanisms for communicating the complexity and contextual nature of the law. As David Dixon points out in the context of custodial investigation, police are rarely informed of

1 The globalisation of policing means that there is constant international sharing of best practice in covert policing methods. This is apparent in Australia with the emergence of the so-called "Canadian model" of using "scenario techniques" to induce admissions: *Tofilau* [2007] HCA 39.

2 S Bronitt, "Entrapment" in P Cane and J Conaghan (eds), *The New Oxford Companion to Law* (OUP, 2008), 381; S Bronitt, "Interpreting Law Enforcement Immunities: The Relationship between Judicial, Legislative and Administrative Models" in S Corcoran and S Bottomley (eds), *Interpreting Statutes* (Sydney: Federation Press, 2005); "Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution? (2006) Vol. 24, No. 4, *Prometheus,* 2006; S Bronitt, "The Law in Undercover Policing: A Comparative Study Of Entrapment and Covert Interviewing in Australia, Canada and Europe" (2004) 33(1) *Common Law World Review* (Bristol, Vathek Publishing) 35-80. http://eprints.anu.edu.au/archive/00002395/

3 A Norrie, *Crime, Reason and History* (2nd ed, London: Butt, 2001), p 19. Bentham's preference for legislation over common law stood in stark contrast to the earlier views of Blackstone who eulogised the common law in *Commentaries on the Laws of England* (9th ed, London: Garland, 1978) (first published, 1765).

judicial decisions, even leading authorities that directly impact on police practices. Indeed, in Australia, police may continue to engage in unlawful processes in one infamous case, relying on dissenting minority opinion in their Police Commissioner Instructions and internal guidelines to 'regulate' their practices. It is clear from the available empirical data in Australia and the United Kingdom that judicial rebukes and even the relatively rare judicial act of excluding evidence on the grounds of investigative misconduct — whether at trial or appellate level — have only limited impact on policing practices.[4]

Another particular problem with appellate court judgments is the issue of publicity – this is when the operational needs of policing collide with the fundamental principles of open justice and the fair trial. The Courts, generally, in weighing the competing public interests defer to operational concerns, though they do scrutinise these claims in the public interest very carefully.[5] In *Tòlifau*, the High Court refused to suppress the details of the operation and police techniques used, noting how extensively the success of the operation and its details had been reported in the press after the initial trial and convictions. Gleeson CJ offered this wry aside about the newly imported 'Canadian' model and the attempts to suppress details of it at that stage:

> … the use by the police of deception in the hope of eliciting admissions is not new. The particular technique of deception adopted in the present cases seems to have been imported into Australia from Canada. Since these trials, it has been reported in the media. Presumably, unless Australians suspected of serious crime are unaware of what is contained in the newspapers, it has a limited life expectancy.[6]

As the Court noted in that case, the practice of eliciting confessions through covert interviewing of suspects had been the subject of several challenges before Australian courts in the previous decade. The leading case on the limits of inducement in the context of covert investigation was *Swaffield* [1998] HCA 1. Although not revealed in the case itself, it is reasonable to infer that the the elaborate scenario testing techniques used by police in *Tofilau* were inspired from training and sharing of 'best practice' received from the RCMP. The police no doubt would have been aware that these techniques had been subject to legal challenges before the Supreme Court of Canada (which ultimately had upheld their constitutionality).

But again there is a problem with this approach to the importation of policing methods from overseas. As Kirby J noted in his separate but concurring judgement,

---

4 For an exploration of the relationship between law and policing from a sociolegal perspective, see David Dixon, *Law in Policing: Legal Regulation and Police Practices* (1997), p 205.

5 This deference to operational concerns appears to be the norm in relation to the police informer privilege: H. Mares, 'Balancing Public Interest and a Fair Trial in Police Informer Privilege: A Critical Australian Perspective' (2002) 6(2) *International Journal of Evidence and Proof* 94.

6 Para [5].

the Charter of Fundamental Rights and Freedoms, with its additional safeguards, has shaped the common law of inducements and the meaning of person in authority in Canada in a distinct way. As Kirby J observed:

> … a literal borrowing of the stated rationale for defining "person in authority" somewhat unsafe. … The *Charter* operates to prevent the admission of statements that "undermine the integrity of the judicial process". This "filter" has no precise equivalent in Australia. Any Australian common law rule must be fashioned without the benefit of access to such a "filter".

Another curious feature of our system of governance flows from the position of police in our legal system.[7] In our system, police are public officers (the office of constable is said to be ancient), but police are *not* servants of the Crown. Civilian police are 'citizens in uniform'. As citizens in uniform they exercise powers that any other person possesses to prevent crime and investigate and prosecute, though they have some specific powers, duties and immunities which parliament has conferred on them (which of course now are extensive). But police are not Crown servants and have a wide independent discretion in how they go about discharging there duties. This is a discretion which the courts are notoriously reluctant to interfere with. The result of this inherited British model of constitutionalism is the police are broadly free to do anything provided it is not unlawful. This point was famously made in the UK case challenging the legality of telephone tapping. Although there was no statutory framework governing its authorisation at that time, this did not render it unlawful. As Megarry VC noted in the case of *Malone* [1979] **344 Ch at** 366-7:

> … there is the contention that as no power to tap telephones has been given by either statute or common law, the tapping is necessarily unlawful. The underlying assumption of this contention, of course, is that nothing is lawful that is not positively authorised by law. As I have indicated, England is not a country where everything is forbidden except what is expressly permitted. … *If the tapping of telephones by the Post Office at the request of the police can be carried out without any breach of the law, it does not require any statutory or common law power to justify it: it can lawfully be done simply because there is nothing to make it unlawful. The question, of course, is whether tapping can be carried out without infringing the law.*

The case ultimately led to Strasbourg and a ruling by the European Court of Human Rights that the absence of any regulatory system – whether administrative or legal – meant that UK law did not prevent arbitrary intrusions into the privacy of its citizens. However, the general philosophical position of the police in that case, constituent with liberal theory, was that the police, like its citizen, are free to do

7 R Hogg, "Criminal Procedure" in T Blackshield, M Coper and G Williams (eds), *Oxford Companion to the High Court of Australia* (South Melbourne: Oxford University Press, 2001).

anything unless prohibited.

This system has some advantages – it provides police with a wide scope of action and indeed an arena for investigative experimentation. Police however need not be rendered figuratively outlaws by this model. In determining how police investigation should be limited it is important to recognise that legal models (based on rules) are not the only, or indeed best, method of regulating investigative power. Legal values, moral principles, human rights and ethics should be used to fill this normative void.

Another Way Forward: Promoting Legal Audacity?

> "It is as much a neglect of duty not to use every lawful endeavour, not to be legally audacious in seeking every investigative tool to bring offenders to justice."
>
> John Grieve CBE QPM, Foreword to the First Edition
>
> C Harfield and K Harfield, *Covert Investigation* (2nd ed, OUP 2009) viii

There is a tendency to view legislation as an improvement on the complex mix of legal and administrative norms that have been applied previously in this field.[8] Adopting this approach, parliament should 'occupy the field' and provide a comprehensive system of regulation of all forms of covert policing not dissimilar to that applied to custodial investigation. In terms of models, Australia could draw on the UK *Regulation of Investigatory Powers Act* 2000 (RIPA). Such an approach would be hugely radical in many respects for Australian police services, which already perceive themselves to be subject to a heavy regulatory burden.

From a philosophical perspective, a statutory framework has the effect of reversing the traditional common law approach to policing, which is that investigators are free to do anything unless expressly prohibited by law. From a realist perspective, a comprehensive administrative framework of governance applied to *all* covert policing, underwritten by law in the same way that telecommunications interception and access is managed, would likely be resisted by police. It would be hard to sell this framework, particularly in the absence of a national human rights charter, which was the stimulus for RIPA in the UK in the late 1990s.

Personally, I am not convinced that importing comprehensive regulation (based on RIPA) would be effective from either a criminal control or indeed human rights perspective. These are burdensome systems of internal administration review and oversight to be sure, but the very nature of these processes means that internal decision-making process can become routinised and may not pass the external "hard look" test. There is also tendency for such models to become a technical question of *legal* compliance, which suppresses the wider moral, ethical and human rights dimensions of policing. As a lawyer, I am concerned about the legal 'tick box' approach to authorisation for covert policing.

While the current system is no doubt flawed in fundamental respects, I am conscious that some features of the existing system are desirable – particularly its

8 C Harfield and K Harfield, *Covert Investigation* (2nd ed OUP, 2008), 9

capacity to be adaptive and innovative around emerging technologies. It has the capacity to produce a form of regulatory dialogue between the legal policy and law makers, courts and the police agencies themselves. In the range of areas I have examined – from entrapment, covert interviewing to ad hoc immunities –there is a complex interaction between regulation by statute, judge-made law and judicial power, as well as internal administrative police guidelines. It is the later arena – the guiding of police action through administrative guidelines - that I believe continues to be largely unexplored territory for the regulation of law enforcement investigative methods in this country. If we move down this route of generating more administrative norms, then there would even be scope for harnessing our specialised tribunal system (Administrative Appeal Tribunals at federal, state and territory level) to determine proactively the legality and propriety of proposed covert action. I have also been attracted by the medical model – the difference between murder and lawful medical procedure can often be a fine legal and ethical line. The medical profession in this country has harnessed law, particularly administrative law, to guide its action in hard cases: seeking declaration about the legality of risky operations. A similar approach could be developed in the covert policing, and would build upon the existing role of the AAT in the issuing of authorisations for telecommunications interception and access of stored data. These tribunals have the advantage that they can draw down on lay members, which often have specialised knowledge (former NCA/ACC lawyers, investigators, and retired police etc).[9] In this respect, a model of investigative powers tribunals available to law enforcement agencies would facilitate a move from the reactive and proactive models of regulatory.

There clearly needs to be more robust and open debate about the role of norms – legal and administrative, internal and external – relevant to covert policing. There has to be a greater preparedness to debate and develop these guidelines in public fora, as they do in the US, UK and even New Zealand – not only will these produce better policing in my view, it would also enhance the legitimacy (and admissibility) of these evidence gathering methods.

9 They are required to act judiciously but are not courts, and therefore do not violate our constitutional separation of powers doctrine which prevents judicial officers being conscripted into Executive roles, like policing and investigating crime.

2

Law Enforcement Agency Use of Covert Powers – Oversight by the Commonwealth Ombudsman

Mr Adam Goodall

Office of the Commonwealth Ombudsman

Abstract

The purpose of statutory audit functions of the kind that the Commonwealth Ombudsman discharges is principally to reassure Parliament and the public that law enforcement powers that are otherwise hidden from public view are being exercised in strict compliance with legislative requirements. Compliance auditing does not stop there. It permits consideration of underlying administrative processes, which can lead to improved accountability and efficiency – a matter of keen interest to the Ombudsman. Compliance auditors are also in a unique position to advise, with both independence and expertise, on the extent to which legislation satisfies policy aims. The Ombudsman can point out to Parliament the practical difficulties created for law enforcement agencies and at the same time make recommendations for legislative change to address gaps in accountability.

As much as the Ombudsman can be critical of agencies and their failure to comply with legislation, an assessment of compliance can be a shield from criticism; from the media, parliamentary committees and other sources. Recognition by agencies of this benefit has led to the Ombudsman being 'invited' to 'look' at certain matters. Such a role is not without problems.

However, there is only so much assurance that compliance auditing can give. The audit functions given to the Ombudsman do not permit the merits of decisions, taken in accordance with legislated process, to be questioned; much less the policy behind the legislation. There are also many practical difficulties that limit the role.

These issues will be discussed in the context of the Ombudsman's oversight of law enforcement agency use of powers under the Telecommunications (Interception and Access) Act 1979, Surveillance Devices Act 2004 and Part 1AB of the Crimes Act 1914.

Keywords: law enforcement agency, covert powers, oversight, ombudsman, compliance auditing, TIA

3

Shifting the Paradigm:Rethinking the Public/ Private Continuum in Covert Private Policing

David Aspland
Charles Sturt University

Abstract

This paper discusses the shift between the public and private sectors in policing, with attention to the covert aspects of the policing function, and why private policing has enjoyed rejuvenation and resurgence over the past 40 years, across the world, after public policing agencies had dominated the field of policing since the early 19th century. It also examines how many aspects of private policing are ideally suited to covert methodologies. It considers the regulation of private policing mainly as it exists in the Australian context, together with issues for Human Rights, especially privacy, in the modern pluralized policing environment. It also examines two key aspects of covert policing by the private sector, the use of CCTV surveillance and Intelligence gathering by paying attention to aspects of Situational Crime Prevention through a number of scenarios. The situation in modern policing is more complex than a simple public/private divide and plays host to a range of interactions that bring many policing actors into contact, competition and alliance in networks and assemblages. Yet most research and regulation still remains focused on public policing even though, numerically, private policing is now a major player in the provision of policing services in an increasingly fragmented, pluralized and commodified market.

Keywords: Covert policing, private policing, security, CCTV, intelligence, privacy, human rights, pluralisation, commodification

1 Introduction

All policing is intrusive given its very nature and covert policing is more intrusive than other models. The actions of policing of all styles infringe of individual rights and freedoms on a day by day basis. Whether it be the right to privacy, freedom of speech or the right to come and go as the individual pleases, the actions of police have the potential to curtail these freedoms. It would be expected though that the infringement of these rights and freedoms is done so for the overall good of the community and with legal authority, justification and accountability. One of the freedoms that is most often infringed upon is the right to privacy. This is done through many forms of surveillance ranging from search warrants, telephone taps, observation, CCTV, video recording and Intelligence gathering.

The common paradigm of policing is that this sort of activity is carried out by properly accountable government agencies with due authority of the law. But is this always the case? In a major shift to this common paradigm, most of this form of infringement of personal freedoms in our society is no longer carried out by government organizations, but rather is carried out by the private sector in an environment where security can be purchased as a commodity (Newburn 2001). The nature of private policing makes it ideally suited to covert, or unobserved, methodologies that sit comfortably with the corporate and consumer driven view of the world, rather than stark uniformed presence. Indeed this is often its main strength in situational crime control.

Yet most research into accountability and regulatory frameworks remains focused on the public police with relatively little carried out into the accountability of private policing or its interaction with public policing (Button 2002 p1)(Hummer & Nalla 2003 p88)(Zedner 2006 p273). Shearing argues that the concentration on public policing has caused a failure of comprehension of the full implications of private policing (1992 p424). What needs to be considered in this debate is the actual accountability of private policing, in all its forms, as much of it falls outside the ambit of state oriented regulatory and Human Rights frameworks (Marx 1987) (Stenning 2009).

A review of current literature points to a commonality of experience across the international spectrum, with private policing organisations expanding worldwide and taking up significant roles especially in the Anglo/American framework (including Australia). Therefore it is useful to draw on material from a range of areas to illustrate the key issues, while remaining focused on the Australian jurisdiction.

The point to start in this analysis is how and why the policing streetscape has changed in the latter 20th and early 21st centuries. A good understanding of these aspects of policing helps to create a greater understanding of modern covert policing forms and methodologies. It also helps to understand why covert policing is the preferred methodology of most organisations involved in private policing. The analysis begins with an examination of the shifting policing streetscape.

2 The Paradigm Shift from Public to Private Policing

Public and private policing have always existed side by side in a continuum. A common misconception is that there remains a strict public/private divide, even if one ever existed. In modern policing there are a range of "assemblages" and "networks" that provide a complex mix of policing interactions and exchanges on many levels (Wood 2006). This has seen services previously provided by government agencies, including policing and security, outsourced completely to the private sector or engaged in joint investigations. There are also private individuals contracting private organizations or organizations where public/private boundaries are blurred and organizations where staff circulate between the two (Marx 1987) (Hoogenboom 2010 p87).

This interaction has not been without its conflict and tensions given the differing cultures and organizational objects of the two sectors. The level of interaction ranges from meaningful and productive cooperation through to deep suspicion and hostility. The past 30 years has seen the rejuvenation of the private policing sector to a point where it now outweighs public policing in many areas by a factor of 2 or 3 to 1. The term "rejuvenation" is used here as prior to the advent of modern public policing in the early 19th century, most policing was carried out by private individuals or organizations. These organizations never went away but were made subservient to public policing organisations authorized by the state for the latter part of the 19th century and for most of the 20th century. They have re emerged in size and number in the late 20th century, to carry out a significant array of policing functions, many of them covert (Shearing 1992)(Hummer & Nalla 2003).

The reasons behind this are varied and complex. There has been an increased demand for policing services driven by many factors including increased fear of crime, insecurity and social unrest; increased levels of actual crime; greater demands for protection caused by increased property ownership created by rising incomes of both individuals and corporations; shifts in public/private space and increases in mass private space. Also there has been a decline in the social "watching" services such as tram, rail and bus conductors and ticket inspectors; roundsmen/women such as milkmen and postal workers; together with other traditional social controls such as churches, schools, neighbourhoods and families that provided much "secondary" social control (Swanton 1993)(Nina & Russell 1997 p7)(De Waard 1999)(Johnston 1999 p179)(Jones & Newburn 2002 p141)(Neyroud & Beckley 2001 p24)(Schneider 2006 p292)(Fleming & Grabosky 2009 p282)(Caldwell 2009 p114).

Since the 9/11 attacks in New York and the beginning of the "War on Terror" there has been an even greater focus on security at all levels. Also, the Global Financial Crisis of 2008, with effects still being realized, has caused significant pressure on governments and a corresponding reduction in public funding for public police (Gill *et al.*2010 p6). This increased demand for policing services has seemed to push public police organizations to the limit of their capacity (Newburn 2001 p841) (Zedner 2006a p153). In fact both public and private policing sectors have increased

significantly in size, but the largest increase has been in the area of private policing. This needs to be viewed as part of a world wide trend across geopolitical boundaries. Sarre (2008) has noted that the private security sector in Australia grew from around 25000 in 1991 to around 50000 in 2006, whereas the numbers of public police increased from 36000 to 42000 in the same period. He further highlights the fact that the increasing demand for policing services has continued unabated into the 21st century.

Simultaneously in the late 20th century, there was a shift to the Neo-Liberal viewpoint in economic policy with an emphasis on "self help" and "responsibilization" (Fleming & Grabosky 2009 p289). This has led to a fundamental reorganization of the policing function and a move away from dependency on state law enforcement (Nina & Russell 1997 p10) (Zedner 2006b p87). Another shift in policing style has been away from the paradigm of "post crime" intervention by the public criminal justice system to the notion of "pre crime" risk management based prevention strategy being more effective (Swanton 1993)(Zedner 2007). This style of crime prevention is very much in tune with the "risk society" philosophy of the Post-Modern world where issues are assessed on the basis of risk management and prevention, rather than solving the crime after the event, which may be virtually impossible in the globalised world of business and travel in the 21st century (O'Malley 2010 p3).

The term "private policing" raises controversy as opposed to "private security" but when the role of this sector is examined as part of the overall social function of "policing" this concept is now greater than just the conventional understanding of "the police" as an organized body in the public domain. Shearing defines the function of policing as "the preservation of peace" where people are free from unwarranted interference to go about their business safely. In this definition he argues against the strictures placed on the notion of "policing" by reference to the activities of the public police (1992 p400). Given this breadth of definition it is logical to expand the concept of "policing" to engage many actors both public and private. These shifts have brought about a situation that may be more suited to covert methodologies than the older "police presence" styles.

It is now true to say that the average member of the public is more likely to come into contact with a private system of policing than a public one in their daily lives (Sklansky 2006 p89). These encounters take place in a wide variety of locations and on a regular basis often without the individual really noticing as they have become second nature. There is the overt presence, whether it is the security guard patrolling at the shopping mall and providing unobtrusive loss prevention services, the security guard at the airport searching passengers as they begin to board their flights or the guard providing security at many government or private buildings where people work. Overseas the use of private security guards has extended into other areas, previously held to be the preserve of public police e.g. in Britain private security personnel have been used to control crowds at public demonstrations and protests (Button & John 2002).

Then there is the not so obvious, covert presence in the form of the CCTV operator, the insurance fraud investigator and the private Intelligence organizations that gather data on other business and individuals. Also much investigation by government agencies in such areas as welfare and taxation fraud is now outsourced to the private sector. Indeed much of what is referred to as "hidden crime" that impacts on our lives is now investigated by private security organisations (Prenzler 2001). As these are not public order issues requiring some form of uniformed presence these areas that are ideally suited to the subtle, persuasive and embedded nature of covert styles of private policing (Shearing 1992).

There have been several descriptions of this phenomenon and one of the most logical is that of the "pluralized" policing environment. Put simply, that means there are now many actors in the policing function. Public policing remains, legislatively and socially, the dominant arm of policing and could reasonably be expected to remain so whilst the nation-state remains the primary political structure. But private policing, in all its forms, is now the largest policing *bloc* in the increasingly fragmented policing streetscape which features a range of public and private organizations offering policing services and interacting on a number of levels. Any consideration of crime prevention strategies in the 21st century, without considering the role and function of private policing, ignores a significant actor in the equation (Hummer & Nalla 2003).

The roles of public and private policing organisations in the area of crime control are intended to be quite different although their ultimate goals can be quite similar in Shearing's definition of social peace (1992 p401). This does not mean to say that there is not now some considerable crossover or roles and functions in the pluralized policing environment. The primary aim of the public police is to keep the peace and uphold the law, whereas the primary role of private policing is to prevent loss to the employer/contractor of those policing services. Also with the move to a globalised world where crime is also becoming globalised and macroeconomic, it is fair to expect that business will also move to seek a globalised crime or loss prevention mechanism that is free of the geopolitical strictures of the nation state. This may be seen an extension of Shearing's "vacuum theory" where private policing continues to exist and flourish in areas where the state cannot guarantee to safeguard the peace and well being of its citizens. In the post-modern, globalised world this may become more the rule than the exception (1992 p406).

3 How is Private Policing Regulated?

This increasingly fragmented and pluralized policing streetscape is becoming more difficult to regulate. This is partly due to the diversified nature of the private security sector. This makes developing partnerships or applying universal standards difficult (Gill *et al.*2010 p29). Prenzler makes the point that it is difficult to prevent misconduct in public policing organizations which are heavily regulated. He goes on to raise the same question with regards to private policing and makes the further

point that in private policing there is a "very high opportunity factor for misconduct" based on "privileged knowledge about clients assets and vulnerabilities, and from the potential 'Dirty Harry' style conflict between noble ends and legal constraints" (2001 p7).

Most scrutiny, research and regulation in policing is focused on the public police, yet some of the larger private policing organizations are more heavily armed and have greater resources than some governments, making them a substantial force in the marketplace. Well run and responsible organizations can be seen to be an aid to government in promoting social and international order, yet they could also become a parallel force operating in a quasi-government fashion contrary to the requirements of elected government and given the sheer numbers of private security personnel now operating in the marketplace, they are significant players in the field.

The American criminologist, Elizabeth Joh, offers a lesson from U.S. history warning against the current enthusiasm for private policing organizations as an alternative to fill the void left by public funding shortfalls. She highlights the great risks for the society concerned if the corporate vested interests that control private policing are not properly regulated. As Marx (1987) points out, the regulatory frameworks in most democracies are aimed at limiting the power of the state over the private citizen but not so much towards what private citizens can do to each other unless that private citizen is in some way acting on behalf, and with the authority, of the government. Shearing advances the idea that it is these experiences in the 19th and 20th Century United States that has coloured the attitudes of much present day analysis of private policing (1992 p405).

The regulation of private policing in Australia relies on state based legislation overseen by the Commissioner of Police for that state and industry codes of practice from industry bodies such as the Australian Security Industry Association Limited (ASIAL). There is also oversight in some states (notably New South Wales and Victoria) from Security Industry Advisory Councils which are made up of key industry stakeholders. Sarre observes that while the role of private policing has increased unabated there is still much confusion over the role and powers of these organizations. He states that the "legal authority, rights and powers of private security providers is determined more by a piecemeal array of privileges and assumptions than by clear law" (2008 p303). There has been little by way of legislation to recognize any special role of the private security industry, with their powers and role still being largely defined as that of the ordinary citizen.

The fragmented nature of the industry also makes it difficult to regulate. There is no one entity that is "private policing". Included in the broad definition are a diverse range of manned security contractors, "in house" security, Risk Consultants, Security Advisors, technical staff and sales people working for any number of organizations ranging from one person, local operations to multi-national corporations. Given the state based nature of regulation staff working for the same company in different states of Australia can fall under different regulatory regimes.

It would be fair to say though that much of the regulation of the industry in Australia is concerned with administrative issues and licencing rather than any ethical concerns of the interaction between the industry and the public (Button 2007 p118). Queensland is unique in having legislated Codes of Practice at this time. However ASIAL provides a number of Codes of Practice that are more specific in dealing with ethical issues in such areas a public interest, integrity, conflict of interest, unethical conduct, surveillance and privacy (2010)(2010a).

Another main basis of the regulation and control of private policing remains the contract between the employer and the private policing organization. It is the employment contract, whether it be for contracted security or "in house" security that defines the role, activities and functions of the security organization or employee and gives them the scope of their authority (Sarre 1994 p263).

Paradoxically, it is this contract based control that can lead to a number of ethical issues as the consumer of these commodified policing services generally purchases these services reluctantly and with a careful eye to the price, rather than quality (Zedner 2006 p271). This creates a downward pressure on costs which leads to low wages and high staff turnover in the private security sector. It also militates against the additional costs of training and accreditation which could lead to a decrease in the professional standards of the industry.

Regulation by customer complaint is not to be underestimated. Given the role of much of private policing is to aid the profitability of the contractor, then the industry can be very sensitive to the needs of customers. This includes both those who hold the contracts and those who interact with private police in retail situations in mass private space, although security guards do tend to act in accordance with private interests rather than in the public interest (Wakefield 2000).

It is in this context that a range of functions are carried out by private police. Wakefield (2000 p126) identifies such functions as housekeeping; customer care; prevention of crime and nuisance behaviour; rule enforcement and use of sanctions; response to emergencies and crimes in progress and gathering and sharing information as key roles in private policing of mass private space. It is in the control of this mass private space that much covert policing is carried out by private policing.

4 Covert Policing by Television - Surveillance of Mass Private Space

The advent of the Closed Circuit Television (CCTV) and its use to monitor public and private space has led to a significant change in policing style in both public and private policing. The use of CCTV has become a critical tool in "situational crime prevention" (Von Hirsch 2000 p59)(Wakefield 2000 p128)(ASIAL 2010a). The extensive use of large numbers of CCTV cameras has allowed for the covert policing and surveillance of large areas of public and private space without the need to deploy large numbers of public or private police in an overt manner with the CCTV seen as a preemptive tool for proactive policing (McCahill 2008). Wakefield

makes the point that the "unremitting watch" of private police using CCTV is often a critical aid to public police in identifying serious offenders (2000 p142).

The sophistication of modern cameras allows the CCTV operator to home in on individuals in a crowd and identify troublemakers. It is a tremendous aid to the crucial power that underpins private policing, the power of exclusion from private property and public/private space (Von Hirsch & Shearing 2000). The main ethical question that underscores the use of CCTV is that it records all persons present in a given area, both persons of interest to the CCTV operator as well as general passers-by and therefore the anonymity of the individual in the public environment has now been greatly diminished, if not removed altogether.

In the public environment it would be expected that the individual has a right to privacy. Article 17 of the International Covenant on Civil and Political Rights provides that no one shall be subject to arbitrary interference with their privacy. It would seem at face value that the random sweep of the CCTV is just such an arbitrary interference. But what of "mass private space" such as shopping malls, which are now becoming the hub of much community life?

The law of property however, when it is applied by private police in mass private space, precludes private citizens from claiming traditional protections to their civil and human rights to a large degree, as put forward in the International Covenant on Civil and Political Rights 1966 (ICCPR) to which Australia is a signatory. When entering mass private space i.e. shopping malls, mass public transport, residential communities, hotel complexes, factories, manufacturing centres, hospitals, office blocks and other areas that could be deemed to be "private property" (Lippert & O'Connor 2006 p57), the citizen loses the right to privacy when having bags or belongings inspected or being under surveillance from CCTV. Gone also is the right to come and go as they please as the greatest power used by private policing is the power of exclusion from private property with dissension regarding the powers of the property owners (or their agents in the form of private security) being resolved by this surrendering of rights being an implied or explicit condition of entry (Sarre 1994 p264):

> *Scenario 1: Duncan Fanning worked as a senior retail loss prevention officer for a large chain of retail stores. During his career he had developed a skilled ability to observe and monitor groups and individuals via CCTV in the various retail centres where he had worked. Most people were in the retail centres to enjoy the ordered atmosphere and shopping that was available. Also however, Duncan had observed a wide range of shop stealing methodologies used by a significant number of individuals and groups. Duncan had made sure that he recorded these methodologies and as many individuals as he could identify. He compiled a database which he shared with other loss prevention professionals, both in the retail store where he worked and other retail outlets belonging to the same chain, and with the public police. In that database he compiled lists of identification, recent photographs available from CCTV, the types of goods favoured, seasonal*

factors and common modus operandi. This information provided a sound basis for Duncan and other loss prevention professionals to exclude "high risk" individuals and groups from the retail centres where they worked.

What this scenario discusses is several of the key issues of covert private policing by the use of CCTV in mass private space; firstly the invasion of privacy and the fact that some people may not wish to be recorded or observed, whilst doing nothing illegal. The CCTV is a "catch-all" technology which is being increasingly widely used and the civil and human rights which underpin our democratic legal system are greatly reduced while the individual is on private property. Von Hirsch points out that this covert surveillance by an "unobservable observer" takes people unawares when they think they are free of scrutiny and that the person can feel constrained by the "chilling effect" of covert surveillance even if this is not the case (2000 p68).

Research shows that the vast majority of Australians (92%) are aware of the use of CCTV in public space and 79% of those surveyed are not concerned with this. Those surveyed suggested a range of public places as being appropriate for surveillance including places where people congregate, public transport and stations, shopping malls and private institutions. Of those that were concerned about the use of CCTV in public places the greatest concerns were that the information may be misused or that it was an invasion of privacy. In spite of this the majority of those surveyed nominated "the police" as an appropriate organisation to have access to CCTV footage, with only a few nominating businesses, Councils or even the organisation that installed the CCTV as being appropriate (The Wallis Group 2007 p74-9)(Hummerston 2007).

Next there is the issue of the power exclusion. This is the main power that private policing holds over the individual in order to ensure compliance although in the private context it can be arbitrarily applied (Wakefield 2000 p133). The power of exclusion is used to remove or restrict undesirable elements from mass private space in order to ensure that the retail trade continues without undue interference. According to Nina and Russell:

'*instead of being concerned about individual civil rights or Human Rights, private security of the "new" public space is more concerned about how to create conditions which can assist in promoting the logic of capital accumulation and the avoidance of any interference in this process'* (1997 p3).

Lastly there is the issue of interaction between the CCTV operator and other agencies in the pluralistic policing environment. What confidentiality requirements are placed upon him/her when communicating observations or releasing video or audio material to other agencies? To what level does this interaction reach? Von Hirsch raises the issue of the risks of unregulated exchanges of information (2000 p70). McCahill also makes the point that the interaction in this environment has assisted the mixing of policing techniques with private police adding "crime fighting " and "law enforcement" to their existing concerns of "private justice" and "loss prevention".

The use of CCTV by security companies is regarded as cost effective and the trend is for a continuing growth in this area (Prenzler *et al* 2009). Walters (2007) states that, based on figures from the Australian Security Industry Association, in the Sydney CBD alone there are some 40,000 to 60,000 cameras and there have also been moves by the NSW State Government, along with many other governments, to compile biometric facial recognition databases for use by police, using photographs collected for drivers licence applications (Jones 2010). The compiling of these databases without public debate raises the issue of what safeguards are in place to protect the use and sharing of these records both now and in the future?

The British experience is even greater than that with an estimated 4.2 million CCTV cameras deployed in the United Kingdom or about 1 for every 14 citizens (Welsh & Farrington 2009 p19). Concerns have been raised about the release and distribution of CCTV footage by a number of agencies as it fundamentally undermines the right to privacy of the individual who may not be connected with the incident being investigated but who may unwittingly appear in the footage (Johnston & Shearing 2003 p69). In addition to the video and audio scanning capacity the British systems also feature sophisticated number plate recognition software that permits large numbers of vehicles to be tracked simultaneously as they travel around major metropolitan areas (McCahill 2008 p215).

The Australian Security Industry Association Limited (ASIAL) website provides a specific CCTV Code of Ethics which states that, among other things, a CCTV is not to be used solely for monitoring and surveillance but must serve a crime prevention function. This is supported by the Office of the Privacy Commissioner, Australia who suggest that the use of CCTV surveillance should have a clear objective and are a proportional response to the defined threat (Hummerston 2007). The possible breaching of privacy by the use of CCTVs is now the subject of reports by the NSW and Australian Law Reform Commissions who recognise that modern technology, whilst a great aid in the workplace, is also a great hazard to confidentiality and privacy (Davitt 2010 p16).

Technology, such as CCTV allows for the covert gathering of a large amount of information on private citizens. This leads to the discussion of another aspect of covert policing by private organisations, the gathering of intelligence.

5 Covert Policing by Intelligence Gathering - Intrusion into Private Lives

Intelligence, the collated and analysed information on which organizations base decisions, is a critical factor in the effectiveness of both public and private of policing. Intelligence gathering is one of the key activities of any form of covert policing. In the digital age it is an area where privacy and policing are often seen to be at odds (Curtis 2007).

The gathering of intelligence on domestic citizens by public policing agencies has been seen both as very necessary, in the context of criminal investigations, to

track both individual criminals and patterns of crime. It is also seen as a threat to democratic freedom as in the stories of Australian Police Special Branches being used to monitor political activists, especially Communists in the case of 1950 and 1960s Australia, and in more recent times, others who were considered unreliable or a potential threat to the established order, until these organizations were disbanded in the mid to late 1990s (Campbell & Campbell 2007 p92). Domestic intelligence gathering by government is now subject to rigorous parliamentary oversight and is highly accountable.

The thought of private companies gathering intelligence on domestic citizens is the stuff of nightmares and conjures up images of an unseen "Big Corporate Brother" watching in a futuristic "Robocop" scenario where all individual privacy has been stripped away by electronic corporate databases and information holdings on individuals. Sometimes this is seen as a threat to democracy itself (Kairys & Shapiro 1980).

Yet intelligence gathering on individuals and organisations has increased dramatically since the 1970s and is carried out every day by hundreds of domestic and international corporations, some as a part of their normal activities while for others it is their sole specialist function. This gathered intelligence is often shared within "Security Intelligence Networks" taking in public and private organisations (Lippert & O'Connor 2006 p 51). If not directly titled *Intelligence* this can go under the names of risk analyses, protective security services or consultancy (Hoogenboom 2006 p375). The use of private intelligence services by corporations stems from issues of cost, need for specialized information to protect business interests (Hoogenboom 2006 p380)(Lippert & O'Connor 2006).

At its most common, the loyalty cards and credit card transactions offered by a wide range of businesses are used to track the spending patterns of clients in order to target them for advertising material and offers. At another extreme insurance companies would hold intelligence information on clients claim histories and assessments on a clients insurance risk as a fraud prevention tool. Button cites examples of private security firms involved in retail loss prevention gathering intelligence on shoplifters and sharing that information with other retail organizations and police in intelligence gathering networks (2002 p104).

Private corporations hold a wide range of information and intelligence on most individuals, ranging from credit ratings, loan default histories through to background employment checks. If one of the primary roles of private policing is to prevent loss for clients, then information and intelligence on potential risks is critical to the success of this role. Lippert and O'Connor (2006) make the observation that whilst private security organisations have developed a significant Intelligence gathering capacity, they tend to share that Intelligence with clients and public police mainly, with only a limited interaction with other corporations, as these are seen as competitors.

Wakefield states that private police, as an aid to situational crime control, can

and do develop risk profiles of individuals and groups in mass private space based on such factors as anti-social behaviour, if they seem "out of place" or they are known offenders. She goes on to point out that much of the activity of private policing in this environment is directed toward gathering and sharing information through such activities as CCTV monitoring, form filling, participating in security networks, engaging in informal liaison with public police and providing information to public police investigations (2000 p139). Some aspects of the issues raised by this are examined in the following scenario:

> *Scenario 2: In a continuation of Scenario 1, along with the lists, Duncan Fanning would provide a range of information from his own experience on the best way to identify and defeat shopstealing groups and individuals, to the other loss prevention officers within his company. At times he would also share this information with the local police, although not to any extent that would cause loss or embarrassment to his employer and only if it was a situation that he could not resolve without the intervention of public police. The information he gathering and analysed allowed him, and his company, to develop proactive strategies in loss prevention based on the methodologies and key times used by the main offenders. This analysis also permitted the extra resources and visible presence of the local police to be harnessed at times of peak risk. However Duncan was reluctant to share this information, on anything but a limited and informal basis, with loss prevention officers from other retail chains as they were competitors in the same field. Also he was aware of issues of privacy that could impact on any formal arrangement.*

This need for information and intelligence has a significant impact in the area of private security as many companies operate without the need for legislative authorisation in many areas, although any organisation dealing in personal information is governed by the Privacy Act 1988 (Hayne & Vinecombe 2008). The issue of the confidentiality of corporate databases and access to client information is one that will bedevil modern society with respect to the privacy of individuals and to what extent does the private security sector have the right to access confidential information, especially if the information has been supplied by the customer to the company, or another company, for alternative purposes than those for which they are being accessed. Williamson highlights the point, in the Australian context, by stating "most organisations do not have adequate governance over the collection, protection and destruction of personally sensitive data" (2010 p12).

In a Review of the Private Sector Provisions of the Privacy Act (Office of the Privacy Commission 2005 p224), the Australian Institute of Private Detectives (AIPD) made a submission asking for private detectives to be considered as a law enforcement body on par with public police. The basis of this submission was that private detectives had limited access to information and that this could prejudice their clients. The submission was refused mainly on the grounds that, unlike public police, private detectives are not accountable to the government or the community

(2005 p229).

Prenzler (2001 p) identified the area of information privacy as a key concern with a number of inquiries taking place in New South Wales and Queensland into the unauthorised trading of information between police, private investigators and their clients (often through "old boy" networks). Prenzler does make the point though that the unauthorised trade could be as much the result of lack of knowledge about the legalities, given the complexity of the regulations governing the sector, as much as any misconduct or wrongdoing (2001 p10). Shearing makes the point that this will arise in situations where former public police join private organizations as a career change and vice versa, as quite commonly happens (1992 p414). This is especially topical given that much data handling is now outsourced to organisations that may not even be within the same national borders. This issue was recently highlighted when a data processing company in India, which processes data from many countries worldwide including Australia, decided to use inmates from a gaol as data entry staff (Farooq 2010).

Gill *et al.* identify the sharing of Intelligence as one of the main stumbling blocks to partnership policing as indicated by a number of senior police officers (2010 p45). In the Australian context there are significant legislative and policy barriers to the sharing of intelligence between public and private policing organizations. Yet the trading and exchange of information within a trusted network is one of the pillars for effectiveness in pluralistic policing (Wardlaw & Boughton 2006 p141). But, whilst many public policing organizations are prepared to accept information and Intelligence, they are unable or unwilling to reciprocate in return and this raises barriers of trust (Harfield & Kleiven 2008).

There are examples of the sharing of information and intelligence between the public and private sectors in law enforcement. Examples of this are the Greater Manchester Community Safety Partnership Team in the UK, the Eyes on the Street Program in WA and Operation Piccadilly to reduce Ram Raids on ATMs in NSW, Australia (Lewis 2008 p158) (Crime and Research Centre UWA 2008)(Prenzler 2009). These may well serve as models for the future.

6 Conclusion

The rejuvenation and expansion of the private policing sector in the late 20th Century leading into the 21st Century has seen private police take up many of the roles previously thought to be the prerogative of the public police. This includes areas of covert policing and has developed to the point where the private citizen is more likely to encounter private policing organizations and forms of policing in their daily lives, than public ones even if they do not realize it. The covert nature of much of private policing means that surveillance and intelligence gathering on private citizens is a fact of life, but the regulation of this area remains fragmented.

This expansion has also led to the situation where the interaction of the public and private sectors of policing is carried out on a daily basis and has led to a re-

evaluation of the paradigm of the public/private continuum in policing. Sometimes this interaction is a beneficial partnership with the sharing of ideas and expertise, other times there is deep mistrust and mutual suspicion between the differing cultures.

While it is believed that public policing will remain the dominant policing form, by virtue of its legislative and social position, private policing will continue to grow and further develop to fill roles and functions required in an increasingly commodified and fragmented policing market. Given the pressure being placed on public policing agencies by ongoing funding and staffing cuts caused by the recent Global Financial Crisis it is likely that this will be the policing model of the future.

References

Australian Security Industry Association Limited (2010). Code of Professional Conduct. 26 November. http://www.asial.com.au/CodeofConduct

Australian Security Industry Association Limited (2010a). CCTV Code of Ethics. 26 November. http://www.asial.com.au/CCTVCodeofEthics

Button, M. (2002). Private Policing. Cullompton, UK: Willan Publishing.

Button, M. (2007). Assessing the Regulation of Private Security Across Europe. *European Journal of Criminology.* Vol. 4. No. 1. pp109-128.

Button, M. & John, T. (2002). 'Plural Policing' in Action: A Review of the Policing of Environmental Protests in England and Wales. *Policing and Society,* Vol. 12, No. 2, pp 111-121.

Caldwell, C. (2009). Reflections on the Revolution in Europe. Can Europe be the Same with Different People in It? London: Allen Lane, Penguin Books.

Campbell, D. & Campbell, S. (2007). The Liberating of Lady Chatterley and Other True Stories. A History of the NSW Council of Civil Liberties. Glebe, NSW: NSW Council of Civil Liberties.

Curtis, K. (2007). The Social Agenda: Law Enforcement and Privacy. *Speech to International Policing: Towards 2020 Conference.* November 20. Australia: Office of Privacy Commissioner.

Davitt, E. (2010). New Laws Needed to Prosecute Invasion of Privacy Cases. *Australian Security Magazine.* January/February. p16.

De Waard, J. (1999). The Private Security Industry in International Perspective. *European Journal on Criminal Policy and Research*. 7. pp143-174.

Farooq, O. (2010). Company Outsources Work to Indian Prison, Plans to Employ About 250 Inmates. *News Limited*. May 13. http://www.news.com.au/business/breaking-news/company-outsources-work-to-indian-prison-plans-to-employ-about-250-inmates/story-e6frfkur-1225865832163

Fleming, J. & Grabosky, P. (2009). Managing the Demand for Police Services, or How to Control an Insatiable Appetite. *Policing. A Journal of Policy and Practice.* Vol. 3., No. 3. pp 281-291.

Gill, M., Owen, K. & Lawson, C. (2010). Private Security, the Corporate Sector and the Police: Opportunities and Barriers to Partnership Working. Perpetuity Research and Consultancy International Ltd.

Harfield, C. & Kleiven, M. (2008). Intelligence, Knowledge and the Reconfiguration of Policing. Harfield, C., MacVean, A. Grieve, J. & Phillips, D. (eds). *The Handbook of Intelligent Policing. Consilience, Crime Control and Community Safety.* Oxford: Oxford University Press.

Hayne, A. & Vinecombe, C. (2008). IT Security and Privacy – The Balancing Act. *Securitypoint 2008 Seminar Series.* February. Australia: Office of Privacy Commissioner.

Hoogenboom, B. (2006). Grey intelligence. *Crime, Law and Social Change.* 45. pp373-381.

Hoogenboom, B. (2010). The Governance of Policing and Security. Ironies, Myths and Paradoxes. Houndmills, UK: Palgrave Macmillan.

Hummer, D. & Nalla, M. (2003). Modelling Future Relations Between the Private and Public Sectors of Law Enforcement. *Criminal Justice Studies.* Vol. 16 (2) pp 87-96.

Hummerston, M. (2007). Emerging Issues in Privacy. *Speech Presented to the SOCAP- Swinburne Consumer Affairs Course.* 2 October. Melbourne. Australia: Office of Privacy Commissioner.

Joh, E. (2006). The Forgotten Threat: Private Policing and the State. *Indiana Journal of Global Legal Studies.* Vol. 13, Issue 2 (Summer).

Johnston, L. (1999). Private Policing in Context. *European Journal on Criminal Policy and Research.* Vol. 7 pp 175-196.

Johnston, L. & Shearing, C. (2003). Governing Security. London: Routledge.

Jones, G. (2010). NSW Government Recording Features for Facial Recognition. Sydney: *Daily Telegraph*, June 3.

Jones, T. & Newburn, T. (2002). The Transformation of Policing? Understanding Current Trends in Policing Systems. *British Journal of Criminology.* 42, pp 129-146.

Kairys, D. & Shapiro, J. (1980). Remedies for Private Intelligence Abuses: Legal and Ideological Barriers. *Review of Law and Social Change.* Vol. 10. pp 233-248.

Lewis, S. (2008). Intelligent Partnership. Harfield, C., MacVean, A., Grieve, J. & Phillips, D. (eds) *The Handbook of Intelligent Policing. Consilience, Crime Control and Community Safety.* Oxford: Oxford University Press.

Lippert, R. & O'Connor, D. (2006). Security Intelligence Networks and the Transformation of Contract Security. *Policing & Society,* Vol. 16, No. 1, March pp 50-66.

McCahill, M. (2008). Plural Policing and CCTV Surveillance. *Sociology of Crime, Law and Deviance.* Vol. 10 pp199-219.

McGinley, I. (2007). Regulating "Rent-a-Cops" Post 9/11: Why The Private Security Officer Employment Authorisation Act Fails to Address Homeland Security Concerns. *Cardozo Public Law, Policy and Ethics.* Vol. 6: 129. pp 129-161.

Marx, G. (1987). The Interweaving of Public and Private Police Undercover Work. Shearing, C. & Stenning, P. *Private Policing.* Newbury Park: Sage Publications.

Newburn, T. (2001). The Commodification of Policing: Security Networks in the Late Modern City. *Urban Studies*, Vol. 38, Nos 5-6, pp829-848.

Neyroud, P. & Beckley, A. (2001). Policing, Ethics and Human Rights. Cullompton, Devon: Willan Publishing.
Nina, D. & Russell, S. (1997). Policing "By Any Means Necessary": Reflections on Privatisation, Human Rights and Police Issues – Considerations for Australia and South Africa. Sydney: *Australian Journal of Human Rights.* No. 7.
http://www.austlii.edu.au/au/journals/AJHR/1997/9.html
O'Malley, P. (2010). Crime and Risk. Los Angeles: Sage.
Office of the Privacy Commissioner (2005). Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988*. Australian Government, March.
Prenzler, T. (2001). Private Investigators in Australia: Work, Law, Ethics and Regulation. *Report to the Criminology Research Council*. Research Project 15/99-2000. July 13.
Prenzler, T. (2009). Strike Force Piccadilly: A Public-Private Partnership to Stop ATM Ram Raids. *Policing: An international Journal of Police Strategies and Management*. Vol. 32, No.2. pp 209-225.
Sarre, R. (1994). The Legal Powers of Private Police and Security Providers. Moyle, P. (ed) *Private Prisons and Police. Recent Australian Trends.* Leichardt, NSW: Pluto Press.
Sarre, R. (2008). The Legal Powers of Private Security Personnel: Some Policy Considerations and Legislative Options. *QUT Law and Justice Journal*. Vol. 8. No. 2. pp301-313
Schneider, S. (2006). Privatising Economic Crime Enforcement: Exploring the Role of Private Sector Investigative Agencies in Combating Money Laundering. *Policing & Society,* Vol. 16, No. 3. September, pp 285-316.
Shearing, C. (1992). The Relation between Public and Private Policing. Tonry, M. & Norval, M. (eds) *Modern Policing.* Chicago: University of Chicago Press. pp399-434.
Sklansky, D. (2006). Private Police and Democracy. *The American Criminal Law Review*. Winter; 43, 1. pp 89-105.
Stenning, P. (2009). Governance and Accountability in a Plural Policing Environment – the Story so Far. *Policing.* Vol. 3. No. 1 pp 22-33.
Swanton, B. (1993). Police & Private Security: Possible Directions. *Trends & Issues in Crime and Criminal Justice.* Australian Institute of Criminology, February.
The Wallis Group (2007). Community Attitudes to Privacy. Australia: Office of the Privacy Commissioner.
United Nations (1966). International Covenant on Civil and Political Rights.
Von Hirsch, A. (2000). The Ethics of Public Television Surveillance. Von Hirsch, A., Garland, D. & Wakefield, A. *Ethical and Social Perspectives on Situational Crime Control.* Oxford, UK: Hart Publishing.
Von Hirsch, A. & Shearing, C. (2000). Exclusion from Public Space. Von Hirsch, A., Garland, D. & Wakefield, A. *Ethical and Social Perspectives on Situational Crime Control.* Oxford, UK: Hart Publishing.
Wakefield, A. (2000). Situational Crime Prevention in Mass Private Property. Von Hirsch, A., Garland, D. & Wakefield, A. *Ethical and Social Perspectives on Situational Crime Control.* Oxford, UK: Hart Publishing.

Walters, C. (2007). There is Nowhere to Hide in Sydney. *Sydney Morning Herald*. 22 September. http://www.smh.com.au/news/national/there-is-nowhere-to-hide-in-sydney/2007/09/21/1189881777231

Wardlaw, G. & Boughton, J. (2006). Intelligence Led Policing – The AFP Approach. Fleming, J. & Wood, J. (eds) *Fighting Crime Together. The Challenges of Policing and Security Networks.* Sydney: UNSW Press.

Welsh, B. & Farrington, D. (2009). Making Public Places Safer. Surveillance and Crime Prevention. Oxford, UK: Oxford University Press.

Williamson, G. (2010). The Problem With Privacy. *Australian Security Magazine.* April/March.

Wood, J. (2006). Dark Networks, Bright Networks and the Place of Police. Fleming, J. & Wood, J. (eds) *Fighting Crime Together. The Challenges of Policing and Security Networks*. Sydney: UNSW Press. pp 246-269.

Zedner, L. (2006). Liquid Security: Managing the Market for Crime Control. *Criminology and Criminal Justice.* Vol. 6. No. 3. pp267-288.

Zedner, L. (2006a). The Concept of Security: An Agenda For Comparative Analysis. *Legal Studies.* Vol. 23. No. 1 pp 153–176.

Zedner, L. (2006b). Policing Before and After the Police. *British Journal of Criminology*. 46. pp 78-96.

4

National Security, Privacy, Ethics, and the Evaluation of Sociotechnical Systems

Lucy Resnyansky
Defence Science and Technology Organisation

Abstract

The use of new technologies of information collection and analysis, and those of surveillance, identification and screening generate numerous debates about their social implications, their effects on individuals' privacy and the balance between governments' power and citizens' freedom.

Another important problem is the moral responsibility of the decision makers and the technology community (both research and industry) as well as the need to consider the society's concerns about security and privacy when specific technological systems are designed, evaluated, and used in particular institutional settings. However, it may be difficult for the designers to think about many social and ethical concerns and problems that may emerge and can become evident in the process of empirical testing.

It is not easy to link concepts belonging to the realm of philosophy and social and legal sciences (ethics, privacy, human rights) with technological ones. Understanding of the elements of sociotechnical systems can be shaped by different disciplinary perspectives and institutional discourses. Therefore, the evaluation of sociotechnical systems should be informed by a critical reflection on the technological vision of the evaluated tools and their use, and on the competing concepts of privacy, identity, and security.

Keywords: sociotechnical systems, national security, privacy, ethics

1 Introduction

> Each technology is multivalent and ambiguous. Both heads and tails are present at the same time. Technology always produces something considered beneficial because it opens options or increases power, speed, or accuracy. But there is also something considered harmful or dangerous for our well-being in the broader sense of the term. (Munoz, 2008, p. 46)

The use of new technologies for information extraction, surveillance, identification and screening have generated debates about their social implications, their effects on individuals' privacy and the balance between governments' power and citizens' freedom (Strickland et al, 2005). An important issue is the moral responsibility of the technology community, as well as the need to answer the society's concerns when technological tools are designed, evaluated, and used in particular institutional settings (Resnyansky, 2010). It may be difficult for technology developers to identify social and ethical issues that may become evident in the process of the tools' implementation and use. It is also difficult to incorporate concepts from the realm of philosophy and social and legal sciences into technological solutions. This paper outlines some conceptual foundations of interdisciplinary research projects aiming to integrate social science knowledge into the development and evaluation of sociotechnical systems. The paper aims to show the importance of critical-reflexive sociocultural analysis in the evaluation of sociotechnical systems by highlighting the different and competing meanings that can be assigned to the concept of privacy.

2 Privacy, security, and technology

Tension has always existed between state interests and individual right for privacy. The new threats, the changing sociocultural context, and technological developments have made this tension more visible and caused the society to re-examine the meaning and value of individual privacy in exchange for promises of safety and security (Strickland et al, 2005). In order to find the best solution, it is necessary to re-examine the concepts of privacy and to redefine them in relation to technology. Different technologies highlight importance of different aspects of privacy. For example, technologies used for physical observation highlight the privacy of as image-based personal information; communication and data storage technologies – the privacy of records; and so on. As noted in Waldo et al (2008), studies of technology and privacy are divided by disciplinary boundaries and aim to address the concerns of specific groups (e.g., civil liberties advocates, regulatory agencies, software developers, health care professionals, e-commerce community, political scientists, and others). These different approaches to privacy need to be integrated, in order "to assess privacy in a manner that accounts for the implications of technology, law, economics, business, social science, and ethics" (Waldo et al, 2008, p. x).

The concept of privacy is linked to specific contexts. Therefore, the privacy/security issue should be approached not as a contestation between abstract principles,

but as a practice that is historically evolving. This evolution includes changes of the range of participants and their activities. In particular, it is important to critically reflect on the fact that the technologist community has developed specific concept of security, privacy and identity. These concepts should not be taken for granted within other contexts, such as National Security. Technology developers and evaluation teams may be willing to address social concerns and answer such questions as: Is individual privacy affected? Is a certain technology-mediated practice socially and culturally acceptable? Are particular groups being discriminated? It may be openly stated that the evaluation of a system should include an assessment of its sociocultural effects. However, it is not easy to transform this general requirement into a set of methodological statements and procedures enabling the team to proceed further than the 'human baseline' (see, e.g., Hall et al, 2007). The concepts of human and social that come from the technologist area have a limited heuristic value for an understanding of the technology's sociocultural effects (Resnyansky, 2010). In addition, the evaluation of a system may be shaped by the market-oriented image of a system that has been skilfully constructed and actively promoted by the manufacturer. The user and the 'target subject' are approached as a 'human factor' rather than participants of a sociocultural process. As a result, the evaluation methodology is shaped – in the best case – by the narrow useability perspective rather than the interests of the broader community.

3 Sociotechnical system as a triadic structure

The concept of the sociotechnical system aims to link the social and the technological. Within the area of organizational development, a sociotechnical systems approach has been used for the design of complex organizational work that is based on interaction between people and technology (Garcia et al, 2006; Luff et al, 2000). Evaluation of sociotechnical systems draws mainly upon Workplace Studies that employ methods enabling researchers to explore the uses and implications of specific systems in specific environments. The methods include an observation of actions and operations, interview with users, videotapes of work processes, and analysis of documents (Jirotka and Wallen, 2000). Within this approach, sociotechnical system is a dyadic structure composed of a piece of technology and a user. The focus is on how the system may affect the user. The main question is how the user (an uncontrollable and unpredictable 'device' attached to the system) can interfere with the performance of a piece of technology. These studies have shown that the development and evaluation of a system needs to be informed by an analysis of the immediate work environment in which the system will be (Bedny and Karwowski, 2007).

The evaluation of systems in an uncontrolled operational environment can also benefit from knowing about sociocultural factors affecting the use and performance of systems (Woodward et al, 2001). The evaluation of systems in operational environment aims to address the following question: Can the system work in the

real world and how efficient is the system in a specific environment? In order to answer this question, a system needs to be conceptualised both in relation to the immediate workplace environment and in relation to the broader sociocultural context. Due to the historical and constructivist nature of sociocultural contexts, it is necessary to explicate different meanings that can be assigned by participants to specific elements of the context and the system. Analysis of the sociocultural context can help technology developers identify a broader range of relevant factors and obtain data that might not be obtained from tests conducted in a laboratory or a controlled environment.

In the National Security context, the sociotechnical system should be approached as a triadic structure (Figure 1). Apart from the user and the tool, it also includes the so called 'target subjects', who are – unless it is proved otherwise – loyal citizens of a democratic state who are entitled to all rights and freedoms, including a right to privacy. The subjects are characterized by multiple, fluid, and contextual social identities, the implication being that their observable behaviour and their perception of the reality can be shaped by different and competing systems of norms and values.

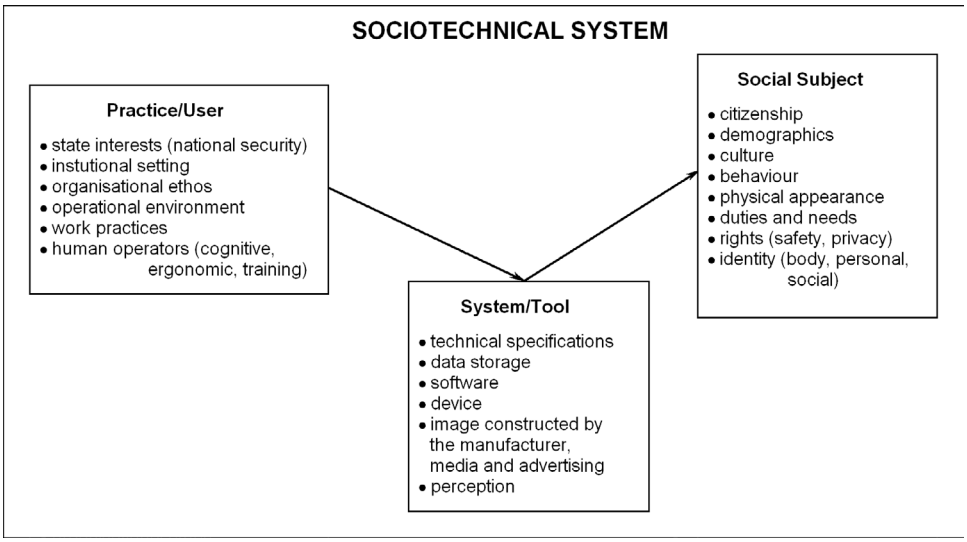


Figure 1 Sociotechnical system as a triadic structure

Sociotechnical systems are shaped by social subjects' vision of the context and other subjects, are embedded in a specific environment and are affecting people, organisations, and society. This concept of sociotechnical systems draws upon the social constructivist tradition in the philosophy of technology and sociology of science, discourse theory, and activity theory (Bijker, Pinch & Hughes 1987; van House 2004). This approach has been applied to the analysis of terrorism models (Resnyansky 2006, 2008, 2009, 2010), and to the study of identification and body screening technologies in security practices (Bennett and Resnyansky 2006; Hall et al 2007; Resnyansky and Bennett 2004). This approach helps understand how the use of technological systems may be affected by the difference between the designer

and the practitioner's visions of a practice.

4 Conclusion

The use of new technologies has generated numerous debates about their social implications, their effects on individuals' privacy and the balance between governments' power and citizens' freedom. On the other hand, there are voices from the technologist community saying that we need to talk "about the engineering aspects of privacy and security, not politics" (Caloyannides 2003, p. 84). Distancing from politics, does not mean that the technologist community has no moral responsibility for the effects of technology. On the contrary, due to the increasing power of technology, the technologist community should take into account the society's concerns about security and privacy. Evaluation of systems is one of the ways in which the society's concerns can be addressed. Consideration of social, legal and ethical issues should become a must in the evaluation of systems aiming to support the National Security practices.

The critical-reflexive sociocultural approach (see also Resnyansky 2008b) provides a foundation for evaluating the sociotechnical systems used within the National Security context as:

- factor of social, cultural and political life. Hence, these systems need to be assessed in terms of their impact on the concepts of privacy, government, identity, and so on;
- tool used for surveillance, screening, identification, information extraction and analysis. Hence, these systems need to be assessed in terms of their effectiveness and impact on workplaces;
- mediator between the National Security practitioners and objects of analysis (people, material objects, and information). Hence, these systems need to be assessed in terms of their possible impact on the practitioners' understanding of the nature of threats, relevance of data and decision-making.

In order to develop recommendations to govern the development of new technological tools and their use within the NS context, it is necessary to critically reflect on the competing concepts of privacy developed within different disciplines and areas of practice. In particular, it is necessary to take into account the changing nature of privacy in the ICTs age, among younger people in particular, and to compare their concept of privacy with the concepts used by the technology developers and technology users. Evaluation methodologies should enable a critical analysis of:

- images of a technological system constructed within the discourses of industry, media, advertising, management, and so on;
- concepts of identity, privacy, and security as linked to specific contexts and technologies
- Empirical data on how specific technologies are perceived by target subjects, and their beliefs regarding the impact of those technologies on the privacy.

References

Bedny, G. and Karkowski, W. (2007) *A systemic-structural theory of activity: Applications to human performance and work design*, Taylor & Francis, Boca Raton, London, New York.

Bennett, P. and Resnyansky, L. (2006) 'How the concept of ethnicity can inform our understanding of the potential impact of security-related technology upon work practices and society', in eds. P. Mendis, J. Lai and E. Dawson, *Recent advances in security technology: Proceedings of the 2006 RNSA Security Technology Conference 19-21 September*, Canberra, pp. 143-158.

Bijker, W., Pinch, T. and Hughes, T. (1987), *The social construction of technological systems: New directions in the sociology and history of technology*, The MIT Press, Cambridge, MA.

Garcia, A.C., Dawes, M.E., Kohne, M.L., Miller, F.M., and Groschwitz, S.F. (2006) 'Workplace Studies and technological change', in ed. B. Cronin, *Annual Review of Information Science and Technology*, *40*, Information Today, Medford, New Jersey, pp. 393-437.

Hall, B., Sunde, J., Johnson, R. and Resnyansky, L. (2007) 'Methodology for the evaluation of sociotechnical systems in an operational environment', *Defence Operations Research Symposium, DORS 2007*.

Jirotka, M. and Wallen, L. (2000) 'Analysing the Workplace and User Requirements: Challenges for the Development of Methods for Requirements Engineering,', in eds. P. Luff, J. Hindmarsh, and C. Heath, *Workplace Studies: Recovering Work Practice and Informing System Design*, Cambridge, UK: Cambridge University Press, pp. 242-251.

Luff, P., Hindmarsh, J. and Heath, C. (eds) (2000) *Workplace Studies: Recovering Work Practice and Informing System Design*, Cambridge University Press, Cambridge, UK.

Munoz, J.M.B. (2008) 'Ethics applied to technologies – Is it well?', *IEEE Technology and Society Magazine*, vol. 27, no. 4, pp. 45-49.

Resnyansky, L. (2006) 'Conceptualisation of terrorism in modelling tools: critical reflexive approach', *Prometheus*, vol. 24, no. 4, pp. 441-447.

Resnyansky, L. (2008) 'Social modelling as an interdisciplinary research practice', *IEEE Intelligent Systems*, vol. 23, no. 4, pp. 20-27.

Resnyansky, L. (2009) 'The Internet and the changing nature of intelligence', *IEEE Technology and Society Magazine*, vol. 28, no. 1, pp. 41-47.

Resnyansky, L. (2010) 'The role of technology in intelligence practice: linking the developer and the user perspectives', *Prometheus*, vol. 28, no. 4, pp. 361-374.

Resnyansky, L. and Bennett, P. (2004) 'Ethnicity in access control and surveillance: Informing Face Recognition System evaluation', Poster presentation at Biometrics Institute Conference, 3 June 2004, Sydney, http://www.biometricsinstitute.org.

Strickland, L.S., Baldwin, D.A. and Justen, M. (2005) 'Domestic security surveillance and civil liberties', in ed. B. Cronin, *Annual Review of Information Science and Technology, 39*, Medford, NJ: Information Today, pp. 433-513.

Van House, N.A. (2003) 'Science and Technology Studies and Information Studies', in B. Cronin (ed.), *Annual review of information science and technology, 38*, Information Today, Medford, NJ, pp. 3-86.

Waldo, J., Lin, H.S., and Millett, L.I. (eds) (2007) *Engaging privacy and information technology in a digital age*, The National Academy Press, Washington, D.C.

Woodward, J.D., Watkins Webb, K., Newton, E.M., Bradley, M., Rubenson, D., Larson, K., Lilly, J., Smythe, K., Houghton, B.K., Pincus, H.A., Schachter, J.M., Steinberg, P. (2001) *Army biometric applications: identifying and addressing sociocultural concerns*, MR-1237-A, RAND.

5

Identity and Biometrics in Cooperative Policing

David Chadwick
Unisys

Abstract

Technology advances in identifying suspects has revolutionised first point of proof procedures in law enforcement. But what are the implications for cooperative policing when used for criminal intent? This paper will explore the issues associated with the civilian use of identification technologies, with particular emphasis on criminal use. Biometric technologies such as facial recognition systems are widely available for purchase and are starting to be used as authentication methods for a number of industries, including nightclubs. But does this open the door for criminal opportunities to start collecting identification material of covert officers? Privacy Act considerations need to be extended to civilian use of biometrics, as well as to Government use.

Keywords: cooperative policing, law enforcement, identify, biometrics, Privacy Act

6

The Covert Implementation of Mass Vehicle Surveillance in Australia

Roger Clarke
Australian Privacy Foundation

Abstract

Automated Number Plate Recognition (ANPR) applies optical character recognition to photographs of vehicles, in order to extract the vehicles' registration data. This paper outlines two alternative architectures for ANPR, referred to as the 'mass surveillance' and 'blacklist-in-camera' approaches. They reflect vastly different approaches to the balance between surveillance and civil liberties. Australian policing agencies have been variously piloting and deploying ANPR, but without public oversight or control. A national agency, Crimtrac, is proposing to develop a vast database, which would store billions of entries showing the whereabouts of vehicles about which no suspicion of wrongdoing exists. Its purpose is expressly to facilitate mass surveillance of the Australian population. This represents national security extremism, and is a gross breach of trust by law enforcement agencies in Australia.

Keywords: ANPR, policing, Crimtrac, national security, mass surveillance

1 Introduction

Automated Number Plate Recognition (ANPR) uses digital cameras and software that provides Optical Character Recognition (OCR) capability to automatically extract the registration data of large numbers of vehicles. The technology is related to, but differs in important ways from, that which has long been used for 'speed cameras' and 'red light cameras'. Background is provided in HTS (2008) and Clarke (2008).

ANPR can be used in a variety of settings, including the entrances and exits of parking-stations, and pricing control-points on toll-roads. It can be applied to parked cars, in order to detect unauthorised vehicles and locate stolen ones.

For traffic management and traffic law enforcement purposes, cameras can be positioned adjacent to roadways, to monitor passing traffic. For minor infringements, it can be used in the same manner as 'speed cameras', as an administrative tool.

For road safety purposes, however (e.g. to assist in catching unregistered vehicles, unlicensed drivers and stolen cars), it is essential that it be used in conjunction with a capability to intercept vehicles of interest. This is a 'real-time location' technology, as that term is used in Clarke (1999a, 1999b). The purposes ANPR is put to may extend beyond traffic matters to policing generally, and to 'real-time vehicle tracking' and 'retrospective analysis'.

In the U.K., police use of ANPR has reached epidemic proportions, has been implemented in an uncontrolled manner, and relies on seriously error-prone underlying data (e.g. Lettice 2005). This has very enormous implications for privacy, and for democratic freedoms more generally. It is crucial that Australian implementations not make the same gross mistakes as the U.K.

This paper focusses on its use by Australian law enforcement agencies, and in particular on the extent to which data is collected and then stored for subsequent analysis. Its purpose is to summarise the position in Australia in relation to ANPR deployments by policing and other agencies, and the subsequent uses of the data that are envisaged by policing and many other law enforcement agencies. The paper reflects research undertaken by the author and other Board members of the Australian Privacy Foundation, in particular APF (2008a) and APF (2008b).

The paper commences by describing the conventional architecture that has been developed and is applied in a number of countries, most intensively in the United Kingdom. The descriptive term 'Mass Surveillance ANPR' is used. An alternative architecture is described, referred to by the term 'Blacklist-in-Camera' technology. This supports targeted use of ANPR for law enforcement, without generating a vast mass surveillance database.

To date, there has been only limited deployment of ANPR in Australia. Current use by policing and other agencies is outlined, shown to have been implemented without public overview or consultation, and shown to use Mass Surveillance technology. A national agency is shown to be seeking to facilitate these implementations, and to warehouse the captured data in what would be the nation's first-ever genuine mass surveillance operation.

2 Mass Surveillance ANPR

A brief description of conventional ANPR architecture is as follows:

> "The ANPR camera-unit can be designed to transmit every instance of vehicle registration-data that it is able to extract from passing vehicles. The receiving device might be a display, for example in a nearby police patrol vehicle. In practice, however, the receiving device is generally a computer with substantial data-storage. The extracted registration-data may be used for user-pays charging and/or law enforcement, ..., but is also stored, together with the date, the time and some indication of location and perhaps direction of view or of movement" (Clarke 2008).

Exhibit 1 provides a diagrammatic overview. A camera captures images that include vehicle number plates. Combined with the camera is one or more processors that extract the number-plate as text, possibly store the image and text, and transmit the image, text and meta-data relating to the image (e.g. date, time and location) to an operational policing hub. The hub selects those that it wishes to intercept and issues alerts to a police vehicle downstream from the wanted vehicle. The hub stores all of the data and/or passes it to a central location for storage and subsequent use.

The effectiveness of ANPR for traffic law enforcement and road safety purposes depends on a large number of factors, in particular the quality of image capture and data-extraction, the speed of alert-generation, the quality of the data on which the alert-generation is based, and the current availability of a suitable resource downstream from the point of sighting.

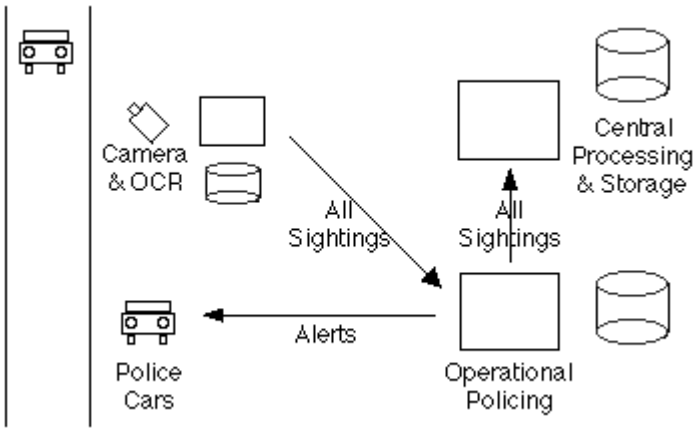


Exhibit 1: Architecture of Mass Surveillance ANPR

The primary focus of this paper is the capture and retention of images and data relating to all sightings, not just the small minority that give rise to alerts. The discussion in (Clarke 2008) continued:

> "Over time, and with the proliferation of image-capture devices, the effect of this process is the accumulation of a massive database of vehicle

> movements. Nothing remotely resembling it has ever existed in the past, even in the old USSR (where internal passports were used to restrict freedom of movement) and East Germany (where monitoring of the population reached its then greatest extremes).
>
> "The justification for such mass surveillance is that there is intelligence value in ANPR data. It might be feasible to locate designated vehicles, to track them in real-time, and to submit vehicles of interest to retrospective tracking. Further, proponents postulate that a wide array of (loose) inferences may be able to be drawn about vehicles being associated with one another in some manner (such as travelling in proximity, or being co-located on multiple occasions).
>
> "Firstly, it is far from clear that any such intelligence benefits are real, and secondly, it appears that national security agencies expect their propositions to be accepted by politicians and the public without supporting evidence, and without question. Even the most cursory consideration of the claims leads to a completely contrary conclusion: vehicle registration data is unreliable, false positives will be frequent, forgery is easy, and both 'organised crime' and terrorists can readily organise themselves so as to circumvent, nullify and even subvert such monitoring".

The deployment of ANPR in the U.K. has expressly been of Mass Surveillance ANPR. See, for example, Lewis (2008). The current project represents the fulfilment of a joint police forces strategy to implement a 24x7 vehicle movement database, in order to "fully exploit Vehicle Intelligence" (ACPO 2005). Exhibit 2 presents the problems with Mass Surveillance ANPR, as summarised by the Australian Privacy Foundation.

3 Blacklist-in-Camera ANPR

The APF's Policy Statement also drew attention to the existence of an alternative way of structuring ANPR infrastructure, which satisfies all of the law enforcement requirements in relation to interception of vehicles, but avoids many of the worst features of Mass Surveillance ANPR.

In verbal evidence, this author described the architecture as follows:

> "the camera has a list of number plates that it is looking for, which may be drawn from multiple sources, of course, depending on what the objectives are. Clearly, motor vehicle registrations that are suspect, that are wanted by police, that have been reported stolen and are not yet reported as unstolen or found, there could be multiples of these lists. But that black list [is] inside the camera, such that the only data that escapes from the camera, [that] is reported to wherever it is reported to, is a hit. ...That clearly would ... avoid all of these problems that arise with a mass surveillance technique gathering large quantities of data about many people's movements" (QT 2008a, pp. 11).

5. As commonly practised, and as supported by currently available technologies, [Mass Surveillance] ANPR represents a gross privacy intrusion, and in some jurisdictions breaches privacy law, in the following ways:

- it involves arbitrary collection of personal data not for a specific, defined purpose to which it is clearly relevant, but opportunistically and for vague purposes
- it generates a very large database of personal data, containing:
    - registration data
    - one set - but very probably multiple sets - of:
        - the date and time of sighting
        - the location
        - the direction of movement
- the database can be used to draw inferences and generate suspicions
- the database is a 'honeypot' that attracts attention from many organisations for many purposes, resulting in 'scope creep'
- the database is impossible to protect against unauthorised access, resulting in leakage of content

6. As commonly practised, and as supported by currently available technologies, ANPR is a mass surveillance technique and breaches the human right of liberty of movement (UDHR 13.1, ICCPR 12.1). More specifically, with conventional [Mass Surveillance] ANPR:

- an unknown proportion of the large data-holdings is unreliable, and there is no simple or inexpensive way of sifting the accurate from the inaccurate
- suspicions can be readily generated, some of which are reasonable and some of which are not, and there is no simple or inexpensive way of sifting the reasonable from the unreasonable
- embarrassment is created for law-abiding citizens who are intercepted on the basis of incorrect data and unreasonable suspicion
- danger is created for law-abiding citizens who are intercepted by a law enforcement officer who has been given wrong information about the possible dangerousness of the vehicle's occupants
- the deterrent effect on miscreants appears unlikely to be all that great
- the unjustified chilling effect on law-abiding citizens appears likely to be much greater than the deterrent effect on miscreants. This applies especially to the many categories of persons at risk, including victims of domestic violence, protected witnesses, celebrities, and undercover law enforcement operatives

7. The practice of ANPR can readily become arbitrary interference by law enforcement officers, in such ways as the following:

- undue interception of false-positives
- misunderstandings, unpleasantness and altercations between officers and vehicle-occupants
- further actions in relation to the intercepted vehicle, such as roadworthiness inspections, bookings for minor transgressions (e.g. broken light-covers and mirrors), and search on the off-chance of finding infringing materials such as drugs
- further actions in relation to the driver, such as delay, questioning and search
- further actions in relation to other vehicle occupants, such as delay, questioning and search

8. The effects of the practice of ANPR on the public reputation of law enforcement agencies and individuals can be positive, in that they will be seen to be active, and to be effective; **but run a great risk of being seriously negative**, in that they will be seen to be intrusive into the activities of law-abiding citizens, and a key part of a 'police state' apparatus that gathers vast quantities of information about people's movements

Exhibit 2: Extracts from the APF Policy Statement (APF 2008b)

A slightly more technical description is as follows:

> "The camera-unit can be designed as a high-security device that only discloses data that satisfies tightly-defined and tightly-controlled criteria. ...Tightly-coupled processing within the camera-unit can compare the registration data extracted from images against one or more controlled blacklists that have been downloaded to it. These can contain the registration numbers of vehicles that law enforcement agencies want to intercept for specific reasons. The only data disclosed by the device would be high-probability 'hits' against those blacklists" (Clarke 2008).

Further key requirements of the 'Blacklist in Camera' design include:

- certified non-accessibility and non-recording of any personal data other than that arising under the above circumstances;
- substantial controls over the download of the blacklist to the device and the maintenance of the blacklist; and
- substantial controls over the quality of data used to prepare the blacklist, and exclusion of sources of data that are of insufficient quality.

Exhibit 3 presents the architecture in diagrammatic form.

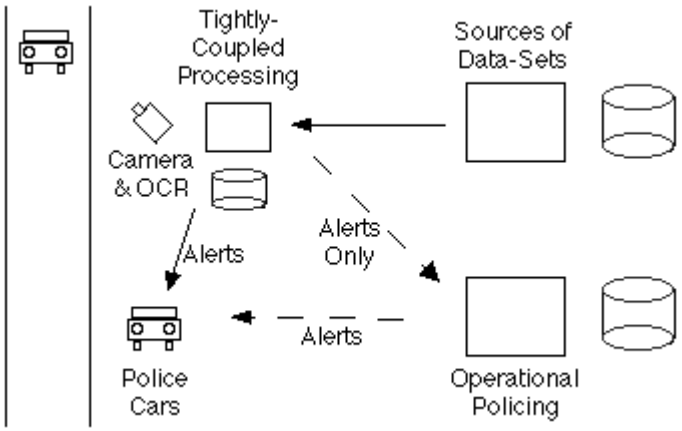


Exhibit 3: Architecture of Blacklist-in-Camera ANPR

Blacklist-in-Camera architecture is not just a theoretical possibility. Applications of it have been in use for some time, at least in various parts of Canada. In a variant in Ontario, for example, "Each licence plate number is transmitted to an onboard computer and immediately compared to the database of stolen vehicles, which is stored on the hard drive of the computer" (OIPC 2003, p. 2). Using this approach the intelligent component of the apparatus, and the database, are in the police-car rather than the camera; but there is still no operational need for the image or the data to be sent to a central point unless it relates to a hit against the blacklist-in-device.

4 Covert Implementation of ANPR in Australia

A number of traffic management and law enforcement agencies in Australia have variously conducted pilots and deployed ANPR capabilities. The first sub-section below provides an overview of these activities. The second sub-section discusses the emergent coordinative mechanism whereby the law enforcement community intends to establish mass surveillance of motor vehicles along similar lines to the rapidly-emergent U.K. "surveillance society" (Ford 2004, HoL 2009).

4.1 Activities of Individual Agencies

This section identifies the extent to which ANPR has been implemented in Australia, and to which the deployments have been the subject of prior evaluation, consultation and authorisation by Parliaments.

4.1.1 Deployments

Predecessor technologies in the forms of 'red-light cameras' and 'speeding cameras' have long been in use in Australia. Capture of an image of a vehicle and its identifier is triggered by an event (variously, detection of a vehicle in a location at a particular time, or moving at a speed, that indicates that a crime may have been committed, or by synchronisation with light-changes from green to amber or amber to red). These give rise to a range of issues (e.g. of accuracy, of data security, and in some cases of automation unmediated by human review). But the issue of mass surveillance does not arise, because no image is captured unless a trigger exists, and a relatively very small proportion of transport movements find their way into a database. ANPR has technical differences from its predecessors. In particular, it necessarily involves digital rather than wet-chemistry photography, and automatic extraction of the registration data in real-time rather than manual and/or deferred extraction.

There have been occasional media releases or press coverage of pilots or initial implementations of ANPR. The primary consolidated sources known to this author are that made available in June 2008 at Appendix 2 on p. 17 of Crimtrac (2008c), mirrored here, and QT (2008b, pp. 5-6). These contain inconsistencies; but it appears that, in most States and Territories, one or more agencies has deployed or at least piloted ANPR, with an apparent total of between 300 and 400 cameras acquired - although not all of them are currently operational. The only longstanding and well-established application appears to be that used by the NSW Road Transport Authority for trucks, called Safe-T-Cam, which operated using older technologies from 1989, but has since migrated from wet-chemistry photography to ANPR. It involves 24 fixed-location cameras, and is to some extent integrated with a South Australian scheme operating a further 11. There is one known instance of the application of the system to cars, in 1998, although the author is not aware of any legal authority for that use (Clarke 2000).

On the basis of the limited available information, it appears that all instances of ANPR in Australia apply Mass Surveillance ANPR architecture. None appear to

use Blacklist-in-Camera technology.

4.1.2 Legal Authority and Public Justification for Deployments

The first and to date only instance of detailed consideration by a Parliament, and of any form of public consultation, was an Inquiry by the Queensland Parliamentary Travelsafe Committee in 2007-08. The 32 Submissions to that Inquiry included two by Privacy Commissioners and two by civil liberties and privacy advocacy organisations - APF (2008a) and QCCL (2008). The Victorian Privacy Commissioner's submission concluded that "The whole concept of an individual's right to anonymity is sacrificed: it is no longer possible to drive on a public road anonymously, even if one is doing nothing wrong" (OVPC 2008, p. 4).

The Federal Privacy Commissioner concluded that (OFPC 2008):

- "ANPR can result in the routine collection of the personal information of large numbers of people. For many of these people, there may be no cause for suspicion and hence no reason to collect information about them. A widespread ANPR system may permit government agencies to track a large number of vehicles (and individuals), revealing where individuals have been, when and potentially with whom. Other than in specific circumstances, this does not seem to be information that government agencies would routinely need to know about members of the community" (p. 6);
- "The Office would caution against establishing infrastructure that could used in such an expansive and invasive manner" (p. 7):
- "The risk of function creep should be managed by:
  - clearly defining the purposes of ANPR technology, and limiting any uses or disclosures to what is reasonably necessary to meet those purposes. To provide for any future purposes that may serve important public interest, a deliberative process should be set out that includes public consultation and parliamentary scrutiny;
  - only the minimum necessary personal information should be collected that is necessary to achieve the stated purposes ...." (p. 10).

The Queensland Parliamentary Travelsafe Committee reported in September 1998 (QT 2008b). It concluded that:

> data concerning all vehicles should not be collected, or should be deleted as soon as practicable without being retained, as the data is unnecessary for that purpose. However, if the purpose of the data collection were to change, for example, if the Queensland Government were to participate in CrimTrac's proposed national ANPR approach, which may include collecting information from all fixed, mobile or in-car ANPR units for interrogation by Australian law enforcement agencies, the change of purpose would first need to be scrutinised by the Parliament" (p. 15);

> "ANPR is being utilised for policing and traffic functions by international and Australian governments, apparently on operational efficiency grounds. Despite the growing usage, there are very few evaluations of its road safety impacts. The committee has cited two evaluations, neither of which could justify the implementation of ANPR-assisted enforcement on road safety grounds" (p. 20);
> "legislation shall prescribe that ... Data relating to vehicles not found to be committing an offence shall be cleansed nightly from devices to minimise the possibility of security breaches" (p. 21). In response to my request for clarification of this point, the Committee Chair wrote that "We could not identify a tangible road safety benefit from the mass storage of ANPR images of motorists going about their private business except where the motorists are actually committing, or are strongly suspected of committing, traffic offences. The only value then in retaining these images is to assist the prosecution of the offences" (Letter of 12 September 2008).

In short, the sole public assessment of ANPR conducted in Australia to date concluded that no justification has yet been demonstrated based on either road safety or even operational efficiency. Hence:

- targeted surveillance of road transport for traffic administration and traffic law enforcement is being introduced speculatively, in the absence of clearly demonstrated net benefits; and
- mass surveillance for purposes unrelated to traffic law enforcement is being introduced, but without justification having been demonstrated.

There are further features of the current situation that give rise to very serious concerns about human rights and parliamentary laxness in exercising oversight over the actions of government agencies. To the best of the author's knowledge:

- with the two exceptions discussed immediately above and below, there is no evidence of any public consultation having been undertaken in relation to any of the many pilots and operational schemes;
- there is no specific authority in law for any of these activities;
- there are no specific statutorily-enforced measures to ensure privacy protection;
- in most cases, the schemes are not subject to general privacy laws (variously because there are none in 5 of Australia's 9 jurisdictions, and because the schemes enjoy full exemption or at least partial exceptions);
- in most cases, any privacy protections that exist are under mere government policies and standards;
- in most cases, any such policies and standards are undocumented or documented in a form that is not publicly available or not widely known to the public (or even the staff who operate the scheme);
- in almost all cases, any privacy protections that exist are essentially unenforceable, e.g. in the case of Queensland, "The committee notes that

the IS42 does not provide any form of redress for individuals whose privacy is breached ..." (QE 2008b, p. 14).

4.2 Coordinative Activities

A wide range of law enforcement agencies exist, in all nine jurisdictions. A key means of achieving coordination among them is Crimtrac, which is a federal government agency formed in 2000 as an instrument of 'collaborative federalism'. Its function is to provide information and information technology services to law enforcement agencies of all jurisdictions, and to facilitate communications among them. Among other services, it operates national fingerprint, DNA and child sex offender databases. Its clientele extends well beyond the policing agencies and the other uniformed services, to many other government agencies in all jurisdictions, and to a range of non-government organisations.

Between early 2006 and late 2008, Crimtrac conducted a $2 million project on ANPR: "The Commonwealth government has funded a scoping study to examine a national approach to ANPR through Proceeds of Crime money. CrimTrac will prepare a report, outlining options and feasibility for a national ANPR capability which will be delivered to the Minister for Home Affairs and the Ministerial Council for Police and Emergency Management - Police by late 2008" (Crimtrac 2008a). As part of the project, consultants were hired to prepare a Privacy issues Analysis, and to conduct a Privacy Impact Assessment (PIA).

A Consultation Paper was provided to a small PIA Consultation Group (Crimtrac 2008c). That Paper stated the assumption that "At this stage it appears likely that the system will collect and store for at least a period all sightings of all vehicle passengers" (p. 6). Further: "there appears to be quite strong agreement [among law enforcement agencies] for the concept of a national APNR system that would make available the combined ANPR data from a range of sources, facilitate information sharing between State/Territory and Australian government agencies and allow searching and analysis of the national set of ANPR data over time", and "All parties considered the system must have the ability to capture data for all passing vehicles through ANPR equipment, rather than just matches against a hotlist" (p. 7).

A 'National Automated Vehicle Recognition System' (NAVR) was envisaged. Key underlying assumptions in the design were (p. 8):

- "data-matching to identify alerts would take place centrally (at agency, jurisdiction or national level) rather than at the camera location;
- "sightings would be collected for all vehicles passing a camera site, would contain an overhead image of the vehicle at sufficient resolution so that the driver or passenger could be identified if appropriate;
- "the system could grow from its current size which is about 300 fixed cameras and 100 mobile cameras to 4000 fixed cameras and 500 mobile cameras;
- "all ANPR data would be held for five years";
- an indicative figure of 70 million sightings per day (implying 127 billion

photographs and associated metadata over a rolling 5-year cycle).

Crimtrac and its PIA consultant were well-aware of the 'Blacklist-in-Camera' alternative architecture when the Consultation Paper was prepared. Among other things, the relevant Crimtrac staff were present when evidence was presented in both written and verbal form to the Queensland Parliamentary Travelsafe Committee (QCCL 2008 and QT 2008a, pp. 10, 11).

In evidence to the Queensland Parliamentary Travelsafe Committee on 14 March 2008, the Crimtrac CEO said that "We have not yet determined exactly the extent to which we would capture all data. It may well be that we only capture hot list data" (QT 2008a, p. 17). Yet only 3 months later, Crimtrac chose to exclude from its Consultation Paper any reference to such a possibility. In short, by the time the PIA was conducted, the 'scoping study' was already fully committed to the facilitation of Mass Surveillance ANPR.

It is unclear whether any written submissions were made during the course of the Crimtrac PIA. None are apparent on the web-sites of the federal, Victorian and N.S.W. Privacy Commissioners. Contrary to expectations, the PIA Report was not published promptly on conclusion of the project, and had not been published at the time of writing in March 2009. The Scoping Study Report as a whole was also due to be completed by late 2008, but neither the Report nor anything about it had been seen publicly at the time of writing.

Crimtrac's CEO, Ben McDevitt, and the Chair of its Steering Committee, Ken Moroney, intentionally created the impression that the agency had an open mind on data capture and retention, and would conduct its study openly, including a full PIA. The agency has abjectly failed to fulfil that commitment. The delays further enhance the opportunity for law enforcement agencies throughout the country to implement ANPR in its mass surveillance form. This creates the likelihood of a fait accompli argument being launched as a defence against public concerns - and, indeed, it is readily inferred that the delays are at least in part intended to achieve that end.

5 Conclusions

A wide array of serious issues arise from ANPR of any kind, including the accuracy of extraction of plate-numbers under varying operational conditions, the accuracy and timeliness of blacklists, vehicle interception procedures, police powers following such interceptions, access to the images and resulting data, the ease and incidence of falsification and duplication of plate-numbers, and the prospect of the onus of proof being inverted and people being required to prosecute their innocence. There is also a concern about the potential for the images to be used to identify people as well as vehicles (e.g. Dearne 2008).

Substantial as those concerns are, they pale into insignificance in comparison with the dramatic change in climate, from a relatively free nation to a 'surveillance society', that is inherent in the implementation of Mass Surveillance ANPR.

During the period 2002-08, the Howard Government dramatically worsened the civil rights / law enforcement powers balance, and significantly reduced the already inadequate controls over the activities of national security agencies (APL 2008). The reputation of the Australian Federal Police is in tatters following its gross over-reaction in the Mahomed Haneef affair, and its inability to acknowledge that errors had been made and to fix the problem (CI 2008). The Rudd Government has provided indications it will do something to restore the balance, by considering the rescission of unjustified measures, and the adjustment of others. After 16 months, however, it has not actually done anything, and the Independent Reviewer of Terrorism Laws Bill 2008 [No. 2] still languishes on the parliamentary table.

ANPR is a litmus test of the Rudd Government's capacity to withstand the backroom pressure put on it by the law enforcement community. The Australian public wants law enforcement agencies to have appropriate technology and appropriate powers; but not to the extent that freedoms and democracy are undermined.

The lack of effective public oversight, the substantial opaqueness of the process, and the long delays in publishing information, lead to the inevitable conclusion that national security and law enforcement agencies in Australia are using covert means to implement mass surveillance of motor vehicles. As expressed by Michael Cope, on behalf of QCCL (QT 2008a, p. 10): "It is a serious concern to us that the creation of this vast database represents a serious threat to privacy and individual liberty. It is really straight out of the Big Brother handbook".

Declarations

In late 2007, this author undertook a consultancy assignment for Crimtrac, through his consultancy company, to prepare a Privacy Issues Paper on ANPR. In March 2008, he was primary author of the APF's Policy Statement on ANPR, and appeared on its behalf before the Queensland Parliamentary Travelsafe Committee. In April 2008, he responded to Crimtrac's invitation to tender for the performance of the PIA, in the process disclosing his absence overseas during part of June and July. The tender was not successful. Because of the potential for conflict of interest, he did not participate in the APF's interactions with Crimtrac during the conduct of that PIA.

Acknowledgements

This paper draws heavily on prior work by the Australian Privacy Foundation. The contributions of (in alphabetical order) Usman Iqbal, Katina Michael, Dan Svantesson, David Vaile and Marcus Wigan are gratefully acknowledged.

Author Affiliations

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra, and is a Board member and currently Chair of the Australian Privacy Foundation. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of

N.S.W., a Visiting Professor in the E-Commerce Programme at the University of Hong Kong, and a Visiting Professor in the Department of Computer Science at the Australian National University.

References

ACPO (2005) 'Denying Criminals the Use of the Roads' Association of Chief Police Officers, March 2005, at http://www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc+ANPR+SITE:acpo.police.uk

APF (2005a) 'Numberplate Recognition Technology' Letter to the N.S.W. Police Commissioner, Australian Privacy Foundation, January 2005, at http://www.privacy.org.au/Papers/NSWPol-Numberplates-050119.doc

APF (2005b) 'Numberplate Recognition Technology', Letter to the Australian Privacy Commissioner, Australian Privacy Foundation, January 2005, at http://www.privacy.org.au/Papers/OFPC-Numberplates-050117.doc

APF (2008a) 'Automatic Number Plate Recognition Technology (ANPR)', Submission to the Queensland Parliamentary Travelsafe Committee, Australian Privacy Foundation, January 2008, at http://www.privacy.org.au/Papers/ANPR-Qld-080118.pdf

APF (2008b) 'Automated Number Plate Recognition (ANPR)', Policy Statement, Australian Privacy Foundation, March 2008, at http://www.privacy.org.au/Papers/ANPR-0803.html

APL (2008) 'Terrorism Law', Australian Parliamentary Library, 2008, at http://www.aph.gov.au/library/intguide/law/terrorism.htm

CI (2008) 'Report of the Clarke Inquiry into the Case of Dr Mohamed Haneef' Commonwealth of Australia, 21 November 2008, at http://www.haneefcaseinquiry.gov.au/www/inquiry/rwpattach.nsf/VAP/(3A6790B96C927794AF1031D9395C5C20)~Volume+1+FINAL.pdf/$file/Volume+1+FINAL.pdf

Clarke R. (1999a) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' Proc. 21st Int'l Conf. on Privacy and Personal Data Protection, pp.131-150, Hong Kong, 13-15 September 1999. Revised version in Information Technology & People 14, 2 (Summer 2001) 206-231, at http://www.rogerclarke.com/DV/PLT.html

Clarke R. (1999b) 'Relevant Characteristics of Person-Location and Person-Tracking Technologies' A separately-published Appendix to Clarke (1999a), Xamax Consultancy Pty Ltd, Canberra, October 1999, at http://www.rogerclarke.com/DV/PLTApp.html

Clarke R. (2000) 'How to Ensure That Privacy Concerns Don't Undermine e-Transport Investments' Proc. AIC e-Transport Conf., Melbourne, 27-28 July 2000, at http://www.rogerclarke.com/EC/eTP.html

Clarke R. (2008) 'You Are Where You've Been Location Technologies' Deep Privacy Impact' Invited Keynote, Seminar on 'Location Privacy', University of N.S.W., 23 July 2008, at http://www.rogerclarke.com/DV/YAWYB-CWP.html

Clarke R. & Wigan M. (2008) 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' Proc. Third Workshop on Social Implications of National Security, Canberra, 23-24 July 2008. Republished in Michael K. & Michael M.G. (2008) 'Australia and the New Technologies: Evidence Based Policy in Public Administration' Research Network Secure Australia, July 2008, pp. 100-114, at http://www.rogerclarke.com/DV/YAWYB-CW.html

Crimtrac (2008a) 'ANPR - Automated Number Plate Recognition' Crimtrac, 2008, at http://www.crimtrac.gov.au/systems_projects/AutomatedNumberPlateRecognitionANPR.html

Crimtrac (2008b) 'Crimtrac Board Considers Number Plate Technology', OnTrac magazine 1, 2 (2008), pp. 10-11, at http://www.crimtrac.gov.au/documents/OnTrac_v1_i2.pdf

Crimtrac (2008c) 'Privacy Impact Assessment Consultation paper: Automatic Number Plate Recognition - CrimTrac Scoping Study' Crimtrac, June 2008, at http://www.privacy.org.au/Papers/ANPR-Background-Paper.doc

Dearne K. (2008) 'Privacy concerns on speed cameras' The Australian IT Section, 23 September 2008, at http://www.australianit.news.com.au/story/0,24897,24387179-15306,00.html

Ford R. (2004) 'Beware rise of Big Brother state, warns data watchdog' The Times, London, 16 August 2004, at http://www.timesonline.co.uk/tol/news/uk/article470264.ece

HoL (2009) 'Surveillance: Citizens and the State' House of Lords Select Committee on the Constitution, February 2009, at http://www.publications.parliament.uk/pa/ld/ldconst.htm

HTS (2008) 'License Plate Recognition - A Tutorial' Hi- Tech Solutions, Israel, November 2008, at http://www.licenseplaterecognition.com/

Lettice J. (2005) 'No hiding place? UK number plate cameras go national' The Register, 24 March 2005, at http://www.theregister.co.uk/2005/03/24/anpr_national_system/

Lewis P. (2008) 'Fears over privacy as police expand surveillance project' The Guardian, 15 September 2008, at http://www.guardian.co.uk/uk/2008/sep/15/civilliberties.police

OFPC (2008) 'Inquiry into Automatic Number Plate Recognition Technology: Submission to the Queensland Parliamentary Travelsafe Committee: Issues Paper No.12 ' Office of the Federal Privacy Commissioner, February 2008, at http://www.parliament.qld.gov.au/view/committees/documents/TSAFE/inquiry/ANPR%20technology/Submissions/28.pdf

OIPC (2003) 'Privacy Investigation: The Toronto Police Service's use of Mobile Licence Plate Recognition Technology to find stolen vehicles' Office of the Information and Privacy Commissioner, Toronto, Ontario, 29 April 2003, at http://www.accessandprivacy.gov.on.ca/english/pir/mun/mc030023.htm, original PDF version mirrored at https://ospace.scholarsportal.info/bitstream/1873/5241/1/10311696.pdf

OVPC (2008) 'Submission for the Travelsafe Committee Queensland Parliament Inquiry into Automatic Number Plate Recognition Technology (ANPR)', Office of the Victorian Privacy Commissioner, January 2008, at http://www.parliament.qld.gov.au/view/committees/documents/TSAFE/inquiry/ANPR%20technology/Submissions/26.pdf

QCCL (2008) 'Submission to the Chair TravelSafe Committee, Parliament House ' Queensland Council for Civil Liberties, 23 January 2008, at http://www.parliament.qld.gov.au/tsafe/view/committees/documents/TSAFE/inquiry/ANPR%20technology/Submissions/24.pdf

QT (2008a) 'Inquiry into Automatic Number Plate Recognition Technology: Transcript of Proceedings - 14 March 2008' Queensland Parliamentary Travelsafe Committee, Hansard, at http://www.parliament.qld.gov.au/view/committees/documents/TSAFE/transcripts/ANPRT%20Transcript%2014.04.08.pdf

QT (2008b) 'Report On The Inquiry Into Automatic Number Plate Recognition Technology' Report No. 51, Queensland Parliamentary Travelsafe Committee, September 2008, at http://www.parliament.qld.gov.au/view/committees/documents/TSAFE/reports/TSR51.pdf

Wikipedia entries:

- Automated Number Plate Recognition - at http://en.wikipedia.org/wiki/Automatic_number_plate_recognition
- Police-enforced ANPR in the UK - at http://en.wikipedia.org/wiki/Police-enforced_ANPR_in_the_UK
- Speed Cameras in Australia - at http://en.wikipedia.org/wiki/Speed_cameras_in_Australia

7

Covert Policing using Unobtrusive Global Positioning Systems Trackers: A Demonstration

Roba Abbas and Katina Michael

University of Wollongong

Abstract

Covert policing is a form of law enforcement focused on the use of hidden techniques, including human intelligence and surveillance, for the purpose of collecting evidence concerning an unsuspecting individual. With the prevalence of Global Positioning Systems (GPS) and associated technologies, agencies are able to exploit the functionality of commercially accessible GPS devices to assist in carrying out such policing activities. This demonstration considers the use of unobtrusive GPS devices for covert policing purposes, with a specific focus on a commercial product named TrackStick Pro.

The study, which is part of a larger project centred on location-based services regulation in Australia, reveals the results of a pilot that examines the steps involved in collecting, downloading, presenting and applying the geographic information gathered from the respective device, as would be the case in covert policing operations. The outcomes draw attention to the ease with which geographic data can be recorded, stored, duplicated and potentially modified. This calls into questison the credibility of GPS-based evidence when utilised by law enforcement agencies. The ability to supplement the location data with additional information, for instance photographs and video footage, is also discussed, as this enables the creation of a single graphical representation of the collated or layered information, allowing for trends to be identified and evidence to be formulated.

Further considerations in the form of privacy, trust and data misuse emerge from this research, given the covert nature of the examined activities. The demonstration will also discuss accuracy with respect to the technical limitations of the device, where issues of inaccurate or incomplete information as the basis of police evidence become problematic.

Keywords: surveillance, global positioning systems, covert policing, location-based data loggers, geographic data, tracking, privacy, trust, data misuse, technological limitations, misinformation

8

For What it's Worth: Cost Benefit Analysis of the use of Interception and Access in Australia

Rob Nicholls

Gilbert + Tobin

Abstract

The thirtieth anniversary of the *Telecommunications (Interception and Access) Act 1979* was one of a number of milestones in 2009. In addition, the regime for access to stored data and delivery of historical and prospective data associated with communication had been in operation for a full year and the Federal Government indicated its commitment to implementing far-reaching amendments to the *Privacy Act 1988* following the Australian Law Reform Commission's landmark report into privacy law.

In this context, the paper examines these developments within the prism of the Attorney-General's 2009 annual report into the effectiveness of Australia's covert telecommunications law enforcement arrangements and with an international comparison. This paper analyses the report in the context of international benchmarks. It does this on a quantitative basis (in terms of cost effectiveness of the regime) and on a qualitative basis (in terms of outcomes compared with the privacy rights foregone). In the quantitative analysis, we consider the cost of the regime per conviction obtained and whether the regime delivers value for money. Our qualitative analysis examines the privacy concerns raised by the regime, particularly in the context of the Australian Bill of Rights debate.

The analysis demonstrates two particularly concerning features of the regime. First, access to stored communications is significantly less effective measured as convictions per warrant than interception. Second, the use of access to prospective data has been significant. The paper concludes by setting out an analysis of the likely compromises required by a Human Rights Act if the current the regime is to remain.

Keywords: interception, access, human rights, warrants, industry practice

1 Introduction

In its first thirty years of operation, the *Telecommunications (Interception and Access) Act, 1979* has moved from providing a strict prohibition on telephony interception (known as wire tapping in the US) to a legislative right of access for law enforcement and revenue protection agencies (Bronitt and Stellios 2005; Bronitt and Stellios 2006; Nicholls and Rowland 2007; Nicholls and Rowland 2008b; Nicholls and Rowland 2008a; Rowland and Alderson 2008). The current legislation permits access to call content on a warrant issued by a member of the Administrative Appeals Tribunal (Bronitt and Stellios 2005) and access to location information of a suspect on the authorization of a bureaucrat (Nicholls and Rowland 2008b). This paper seeks to consider whether the effects of this regime represent appropriate value for Australians by considering both the financial and privacy costs.

The approach that is taken in the paper is to present and analyse the results of the legislative regimes for interception in each of Australia, the UK, the US and Canada and to consider whether the effects of human rights in each country has a specific impact on the balance between the needs of law enforcement agencies and the privacy of the individual. We do this by first outlining the preferred model for enshrining human rights in Australia before examining the results of the legislation in that country. We then move on to examine the outcomes of similar legislation in the case study countries and note why there may be differences in the outcomes. We conclude by considering the likely effects on the current Australian legislative environment of a Human Rights Act. We suggest that the current outcomes would likely be affected by any form of change (legislative or constitutional) which has the effect of ensuring that either privacy or an assumption of innocence are regarded as fundamental human rights which cannot be extinguished by legislation.

2 Human Rights in Australia

Australia does not have a constitutionally provided set of human rights at a federal level. Australia is a signatory to the United Nations Convention on Human Rights and each of Victoria and the Australian Capital Territory have human rights legislation. This legislation is *Charter of Human Rights and Responsibilities Act 2006* (Vic) (**Victorian Charter**) and *Human Rights Act 2004* (ACT) (**ACT Charter**). In December 2008, the Australian federal government launched a national public consultation on how best to promote and protect human rights and responsibilities in Australia. The independent committee appointed by the government was charged to consult broadly with the Australian community and consider whether Australia should have a federal Charter of Human Rights.

For the purposes of this paper, we will consider the potential impact of enacting a federal Charter of Human Rights, which is similar to that in the comparable jurisdiction of Victoria. Such a Charter would provide a human rights framework for the operation of the federal public sector with respect to those human rights set out in the Charter and place the following obligations on the arms of the federal

government (Williams 2007: 83-85):

- **Executive:** Public servants, government departments and other 'public authorities' would be required to apply existing government policy, and develop new policies, compatible with those human rights set out in the Charter (Williams 2007: 84). In addition, *"it is unlawful for a public authority to act in a way that is incompatible with a human right [set out in the Charter] or, in making a decision, to fail to give proper consideration to a relevant human right"* (section 28 of the Victorian Charter). This would not in itself create any independent cause of action or relief or provide a freestanding right to recover damages in the event of a breach of a human right set out in the Charter. However, it may be used as a further ground in an existing cause of action for unlawfulness of that 'public authority', in particular administrative review and injunctive relief are possible (section 39 of the Victorian Charter and Williams 2007: 84).
- **Legislature:** Each Bill introduced into Parliament would be accompanied by a statement of compatibility setting out with reasons, whether in the opinion of the parliamentarian introducing the Bill, it is compatible with those human rights set out in the Charter and the nature and extent of any incompatibility (section 38(1) of the Victorian Charter). Parliament may still pass the Bill, even in the event of incompatibility.
- **Courts and Tribunals:** All statutory provisions would be interpreted in a way that is compatible with the human rights set out in the Charter, *"so far as it is possible to do so consistently with their purpose"* (section 32(1) of the Victorian Charter). Where a statutory provision cannot be interpreted in a compatible way, then the matter may be referred to a higher court which can declare an inconsistent interpretation (section 36(2) of the Victorian Charter). This does not *"affect in any way the validity, operation or enforcement of the statutory provision"* (section 36(5) of the Victorian Charter), but requires the responsible minister to provide a written response to parliament. Parliament then has the final say as to whether to amend the law or not.

The types of rights which would be protected as part of a Charter at a federal level would include the right to privacy as well as the right to a fair trial (and the associated presumption of innocence, or at least, non-guilt) (Johnson and Santow 2009: 6). However, we note that the likelihood of the introduction of human rights legislation is unlikely in a period of minority government.

3 The Interception Regime in Australia

In Australia, the Attorney-General is obliged to report each year on the use of warrants for interception of telephone calls and warrants for access to stored communications (Attorney-General 2009). Broadly, there is a strict prohibition against call monitoring and a limited immunity is provided in respect of that prohibition if a warrant is in force. On this basis, telecommunications carriers execute warrants when they are served by the relevant agency. In the period from 1 July

2008 to 30 June 2009, there were more than 3,500 warrants executed in Australia (split between interception and access). The split between the offences reported by the Attorney-General is provided in the report and reproduced in graphical form in Figure 1 and Figure 2.

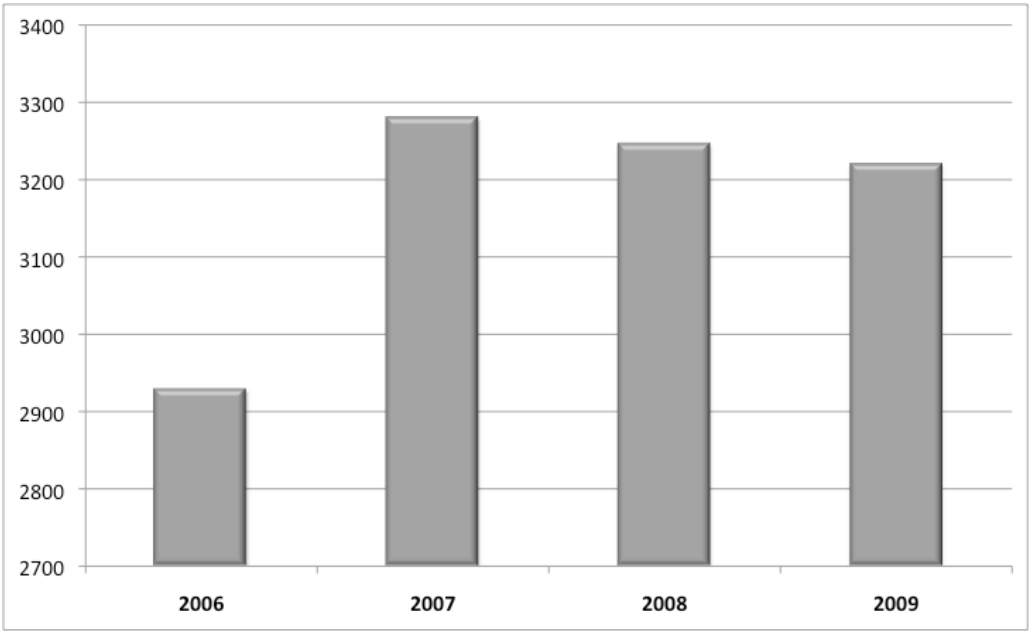


Figure 1: Total interception warrants in Australia

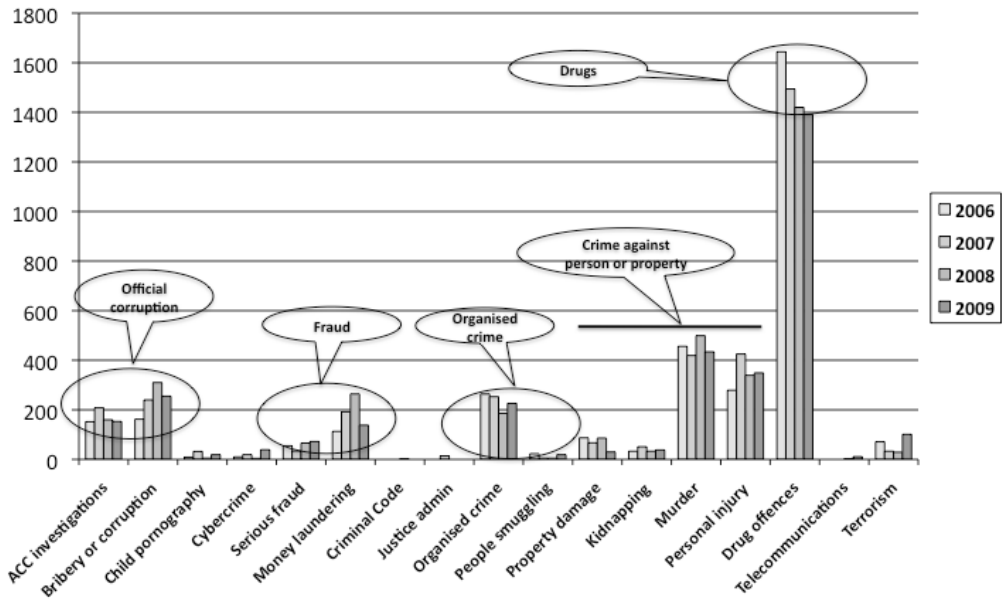


Figure 2: Interception warrants in Australia

Figure 1 and Figure 2 also set out the figures from the previous three years. It can be seen quite clearly that the major criminal activity for which interception of calls is used is drug offences, which account for nearly half of all warrants. The diagram has also grouped other crimes to assist in the analysis of the use of warrants. The striking features of the longitudinal information are the similarities between the number of warrants over the period set out in the graph and by offence.

When an interception warrant is drafted, the length of the interception is stated on the face of the warrant. The actual duration of the interception is typically a shorter period as an amending document which halts the application of the warrant is typically sent before the period stated on the warrant expires. This is reflected in the data set out in Figure 3.

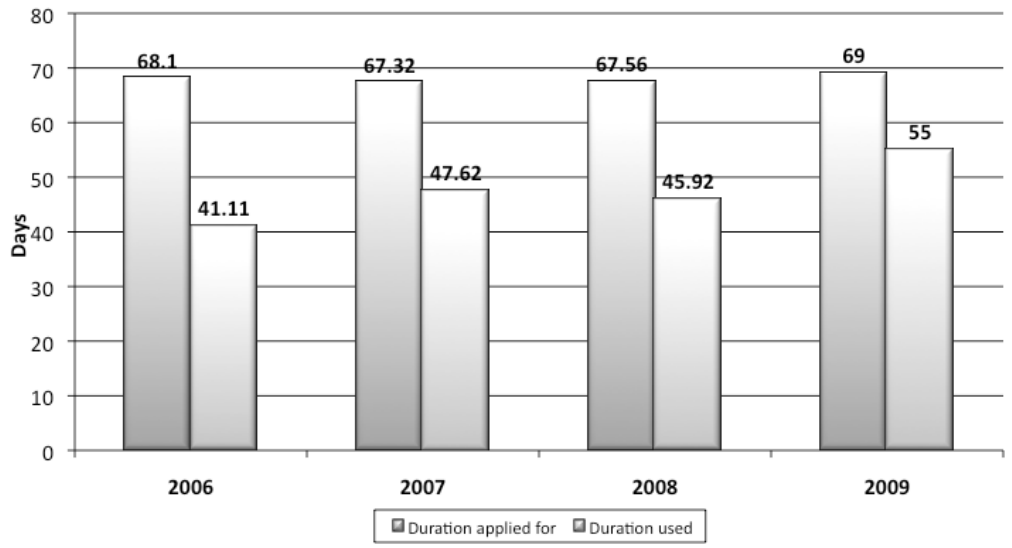


Figure 3: Duration of interception warrants in Australia

The reason for providing this data in the paper is to provide a comparison to the duration of warrants in other jurisdictions below.

The Attorney-General's report also provides information as to the costs incurred by each agency in the warrant process. As information is provided on the total costs and total number of warrants, it is possible to calculate the total cost per warrant. The report also does this calculation in respect of the cost per warrant by agency. The overall result is set out in Figure 4.

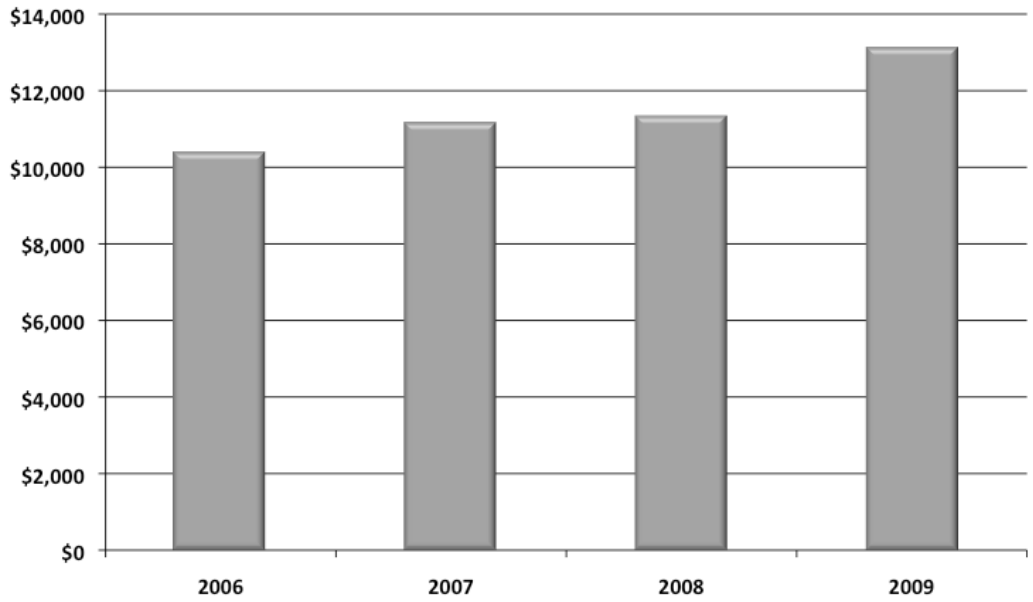


Figure 4: Cost per interception warrant in Australia

It is important to note that the change in the per warrant cost (expressed in Australian dollars) has not changed very significantly over the three year period shown, although 2009 is higher than the average of the previous three years.

We now turn to the key question in respect of the telephone interception regime – does it produce results? The answer to this is set out in Figure 5.

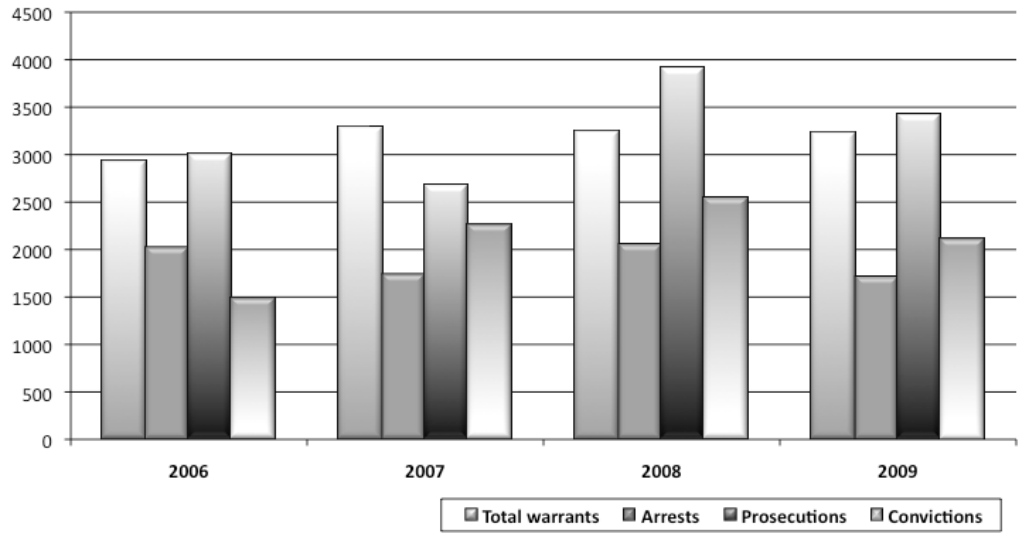


Figure 5: Effectiveness of interception warrants in Australia

Figure 5 demonstrates that there is a reasonable level of effectiveness of interception warrants. In broad terms, the number of arrests per warrant is greater than 50% and this level is relatively constant. The number of prosecutions is higher than the number of arrests, but this may reflect the fact that there is a likelihood that each arrest which leads to a prosecution leads to prosecution for more than one offence. The number of convictions per warrant has risen over the period from 2005/2006 to 2008/2009 and, given that there has been a more modest increase in the per warrant cost in that period, the interception warrant regime is showing a lower interception cost per conviction over time.

The picture in respect of the stored communications access regime is set out in Figure 6.

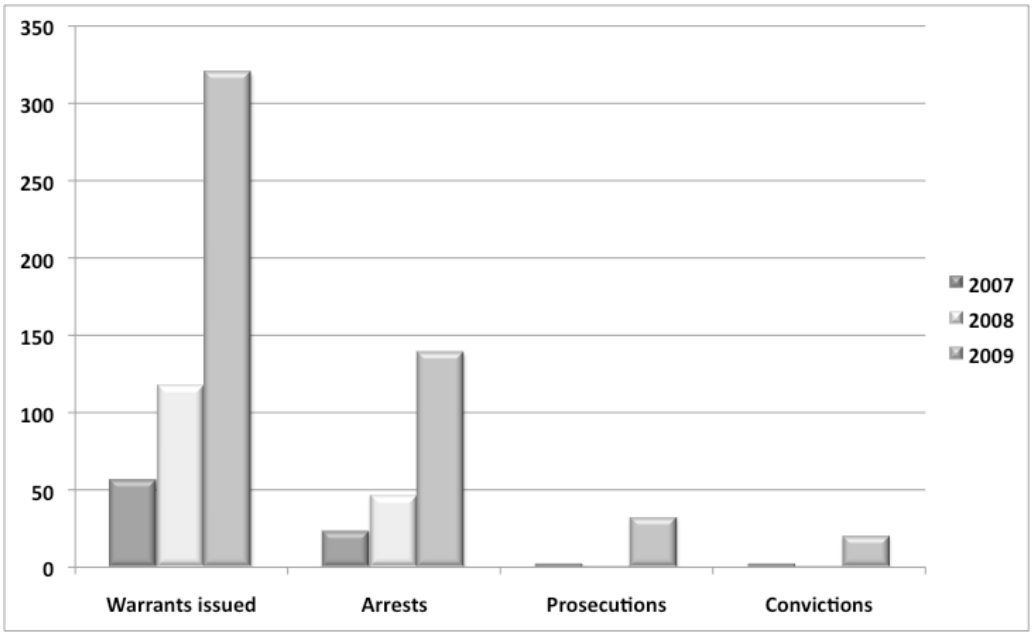


Figure 6: Effectiveness of stored communications warrants in Australia

There were 117 warrants applied for in the first full year of the regime. As a result of these warrants, there were 46 arrests. Based on the interception statistics set out above, this would be considered reasonable. However, the Attorney-General reports only a single conviction. This would not be problematic of itself. After all, the regime is new and it could be that prosecutions may be pending. However, with no reference to privacy or fair trial concerns, the Attorney-General's report notes, "Many enforcement agencies do not have prosecutions and convictions as a primary aim". In 2009, the conviction to warrant rate had improved, but is still well short of the level that is achieved in the interception regime.

Operating in parallel with the interception regime is an obligation on carriers and carriage service providers to provide reasonable assistance, on request, to law

enforcement agencies and revenue collection agencies. There were more than a quarter of a million of these requests in the year to 30 June 2009. This figure was up 34% over the previous period. Of these, 245,297 related to criminal law and 7,014 related to other matters. In perspective, this represents a request to population ratio of greater than 1%. Given that each request leads to call records being provided (broadly, the calling and called party along with time, date, duration and type of call). This data would have included information that would have been regarded as private by a large number of parties who were not the subject of investigation.

In addition to the assistance that was rendered through the supply of historical data, there were also requests for "prospective" or near real time data. This data can include real time location data (from mobile targets) as we have previously described (Nicholls and Rowland 2008b). In the first year of operation, there were 1,315 such requests each with an average 18 days in force and an average 29 days applied for. In the 2009 report period, the number of requests had nearly doubled to 2,571 with an average 23 days in force and an average 30 days applied for.

4 The Interception Regime in the USA, Canada and the UK

The USA reports interception matters on an annual basis (US Courts 2010). These data are based on warrants issued in Federal and State Courts on behalf of law enforcement agencies and cover the period 1 January 2008 to 31 December 2009. The statistics provided do not include interception related to homeland security or issued in accordance with the Patriot Act and are thus understated. Nevertheless, the most striking statistic from the USA is the fact that the total number of warrants was a little over two-thirds of the number in Australia (despite the population of the USA being some 15 times greater than that of Australia). Set out in Figure 7 is a graph of the total number of warrants over a thirteen-year period split between Federal and State.

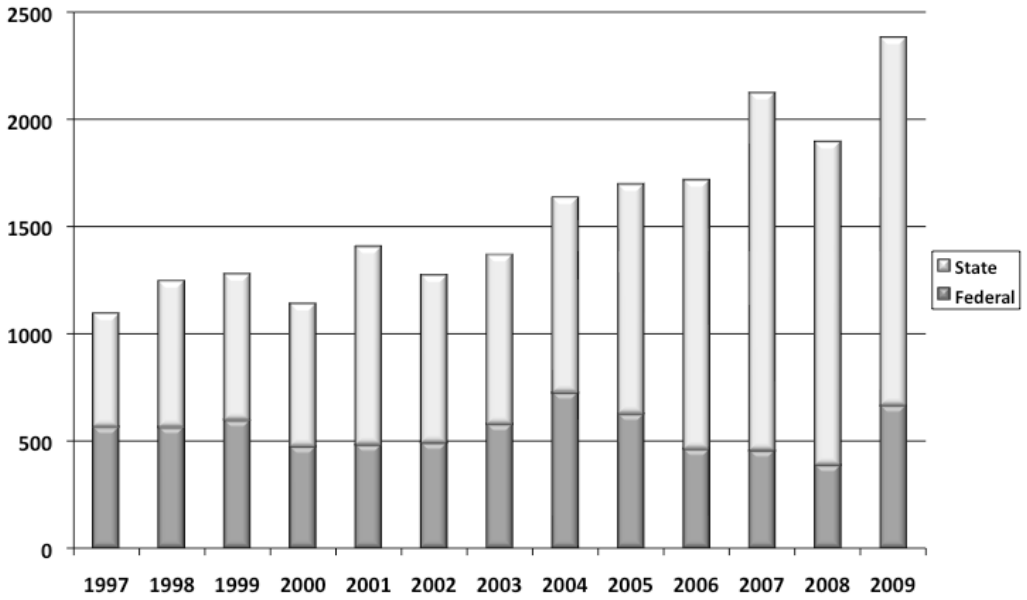


Figure 7: Communications interception warrants in USA

The majority of warrants reported were for offences in relation to drugs and this is graphed in Figure 8.

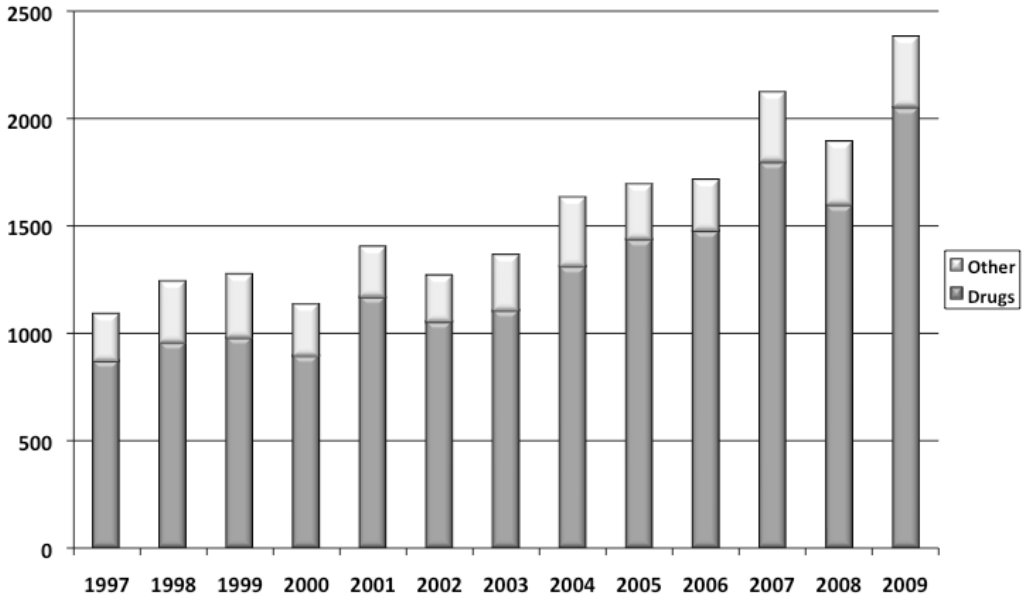


Figure 8: Communications interception warrants in USA

There average length of a warrant is comparable to Australia (with an average duration of 42 days – up from 41 days in 2008). However, the attributable costs in

the USA are significantly higher at $US52,200. The associated arrest rate in the USA is higher than in Australia at 4,537 people but the number of convictions as a proportion of interception warrants is lower with 678 convictions in the US in the 2009 reporting period.

In Canada, the annual report on interception is made under the Criminal Code and covers the period in the calendar year (Canada 2010). The 2010 report is in respect of 2009 and separates telecommunication interception warrants from other listening devices. The number of warrants issued was slightly greater than 13% of the number issued in Australia (despite Canada's population being 50% greater than Australia's). The number of warrants is declining over time and this is set out in Figure 9.

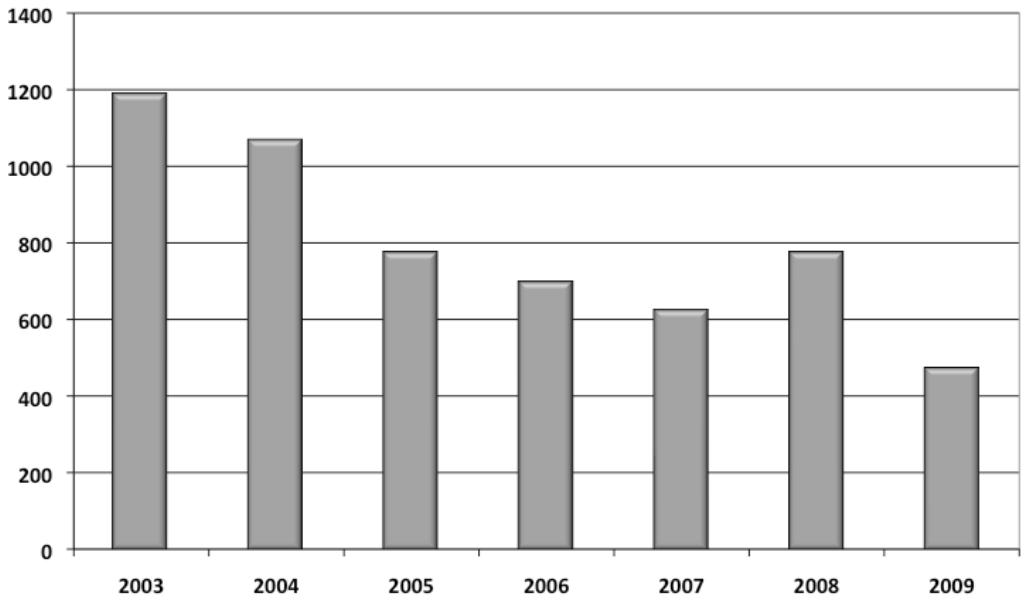


Figure 9: Telecommunications interception warrants in Canada

There is a specific reason why the Canadian regime may have fewer warrants per capita than Australia. In Canada, the target of an interception warrant must be informed of the prior existence of the warrant. This can be as a part of the prosecution process if the case goes to court. However, if the case is not prosecuted, the target must also be informed. It is likely that this human rights protection reduces the number of warrants applied for by the law enforcement agencies.

In the UK, there is an Interception of Communications Commissioner, appointed by reference to the Human Rights Act, who reports on the interception of communications on an annual basis (Interception of Communications Commissioner 2010). This report excludes Northern Ireland. However, the total number of warrants was about half that of Australia for a population which is about three times

greater as set out in Table 1.

Responsibility	Number in 2007	Number in 2008	Number in 2009
Home Secretary	1,881	1,508	1,514
Scottish Executive	145	204	192
TOTAL	2,026	1,712	1,706

Table 1: Interception in the UK

There are also reasons why the UK statistics would indicate a lower use of warrants on a per capita basis than in Australia. The call content of interceptions cannot be used as direct evidence in the UK. As a result, the value of the call content to law enforcement agencies may be lower than it is in Australia. This is suggested by the 525,130 requests for communications data in 2009 (which is two-thirds of that in Australia in per capita terms). On the other hand, another reason for the lower number of warrants on a per capita basis may be the effects of the Human Rights Act in the UK.

5 The Effects of a Federal Charter and Conclusions

We now turn to the likely impact of either a federal charter of human rights or a Human Rights Act in Australia. It seems likely that there will be a need for a "Human Rights Impact Statement" to be issued for review by the Parliament when each new proposed piece of legislation is considered and debated. In recent years, the *Telecommunications (Interception and Access) Act 1979* has been amended regularly – more often than annually over the period 2005 – 2009. Each time that amending legislation is introduced, the Minister (in this case the Attorney-General) will need to be certain that there is no adverse effect on human rights or will have to disclose to the Parliament what that adverse effect will be. It is unlikely that the Attorney-General will be able to argue to the Parliament that the need for interception will not be balanced by convictions (as we quoted above).

At the moment, particularly in relation to prospective data, senior officers have an obligation currently to "take into account" the privacy of targets. In an environment where there are enshrined human rights, the same officers will be under an obligation to take into account the target's basic right to dignity and ability to take part in society. This is likely to be a higher threshold and may reduce the number of requests (and, potentially, warrants).

The final issue is the extent to which firms will reconsider the term "reasonably necessary" in the context of human rights. In Australia, the same carriers upon which the law enforcement and revenue collection agencies rely for assistance have been among the first firms to support a new human rights framework. Although any such framework will not automatically bind firms, it is likely that a significant number of firms, particularly carriers, will choose to "opt-in" to a charter of rights. In that position, they may argue that assistance to agencies in certain circumstances

would be adverse to human rights. As set out above, the interception regime in Australia is based on limited immunities from a strict prohibition. Firms may take the view that immunity in relation to one piece of legislation is not sufficient for action which would contravene an individual's human rights, set out in another. Perhaps in the context of human rights we will move to a situation where the number of warrants for interception in Australia will not be at an annual level which is comparable to the sum of the number of warrants in the USA, Canada and the UK, each of which have human rights protection enshrined in either the law or the constitution.

Acknowledgements

The Author would like to thank Katina Michael and Simon Bronitt for organizing the workshop "Social Implications of Covert Policing" at the ANU in April 2009 and for the feedback given there to an earlier version of this paper. In particular, the feedback from Nick O'Brien of Charles Sturt University has been incorporated into the drafting of this paper. This paper was produced when the author was at Gilbert and Tobin. The firm, especially Michelle Rowland, provided significant help in formulating the paper. Francine Johnson from the Gilbert + Tobin Centre for Public Law also provided assistance on the likely form of human rights enactment in Australia.

References

Attorney-General (2008). Telecommunications (Interception and Access) Act 1979: Annual Report for the year ending 30 June 2008. Canberra, Attorney-General's Department.

Bronitt, S. and J. Stellios (2005). "Telecommunications interception in Australia: Recent trends and regulatory prospects." Telecommunications Policy 29: 875-888.

Bronitt, S. and J. Stellios (2006). "Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?" Prometheus 24(4): 413-428.

Canada (2010). Annual report on the use of electronic surveillance. Ottawa, Public Safety Commission

Interception of Communications Commissioner (2010). Report of the Interception of Communications Commissioner for 2009. London, UK Government.

Johnson, F. and E. Santow (2009). Would an Australian Charter of Rights be good for business? Position Papers: Gilbert + Tobin Centre of Public Law, UNSW. Sydney, Gilbert + Tobin Centre of Public Law, UNSW.

Nicholls, R. and M. Rowland (2007). Message in a bottle: Stored communications interception as practised in Australia. From Dataveillance to Überveillance and the Realpolitik of the Transparent Society: The Second Workshop on the Social Implications of National Security. M. Michael and K. Michael. Wollongong, Wollongong University.

Nicholls, R. and M. Rowland (2008a). Lost in transcription: The Australian regime for interception of, and access to, communications content and metadata. Communications and Policy Research Forum, UTS Sydney, Network Insight Institute.

Nicholls, R. and M. Rowland (2008b). "Regulating the use of telecommunications location data by Australian law enforcement agencies." Criminal Law Journal 32(6): 343-350.

Rowland, M. and S. Alderson (2008). "New telecommunications interception and access proposals: the first or last of many?" Communications Law and Policy Bulletin(May 2008).

US Courts (2010). Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications. 1 January 2009 - 31 December 2009. Washington.

Williams, G. (2007). A Charter of Rights for Australia. Sydney, UNSW Press.

9

Avoiding a Privacy-Security Telecommunications Deadlock Under Emergency Declarations

Anas Aloudat
University of Wollongong

Abstract

Australian political efforts with relation to security in the past few years seemed to be progressively characterised by the emergence of shared global risks, in a manner we started to observe unprecedented measures forcefully attempted to counter the growing threatening potentiality of all identifiable man- and natural-caused risks. As the consequences of these complex risks have the intrinsic capacity to effect severely on societies, and not merely on individuals, governments' accession to these socially constructed measures have been presented to the public as an absolute necessity to sustain the uninterrupted order of today's civil society. At the same time, however, these measures have been perceived by many as a substantial move towards the curtailment of privacy rights and the beginning of a gradual introduction of blanket covert/overt policing practices on every aspect of our lives, leading down the path towards a complete surveillance society. Driven by this, the paper takes a look into some of the implications of the Australian government's anticipated decision to deploy a nationwide location-based mobile phone emergency warning system and discusses what would arguably initiate a possible privacy-security telecommunications deadlock, evoked by the temporary waiving of the right to privacy under emergency declarations under which the warning system would be primarily utilised. The paper provides few recommendations to partially help avoiding a possible deadlock and finding some sort of balance between security and privacy in the context of emergencies.

Keywords: Privacy, security, telecommunications deadlock, personal identifiable information, emergency warning system, location-based service, securitisation.

1 Introduction

Emergencies are inevitable situations in the continuum cycle of life and death. Some of these most extreme natural- and man-caused events showed us that no country in the world is immune to their impact. September 11 New York attacks, the 2004 Indian Ocean Tsunami, the 2005 Hurricane Katrina, and the recent bushfires in Australia in February 2009, are just a few examples of what could societies suffer, regardless of the technological advances the nation is achieving.

The complexities of these events, their surrounding uncertainty, timing and severity have significantly helped paving the legislative ways for proposing and deploying of vigorous unprecedented security measures meant for a better preparedness, protection and response to their threatening potentiality. As a direct result of these security measures and because of the global political climate several countries, including Australia, have headed in the past few years for what can be framed as the inclusive securitisation of the whole society.

Although the focus of securitisation is on counter-terrorism measures, the processes fundamentally cover any related enactment, policy, legislation or action taken by the forces in power to increase the levels of security in an attempt to reduce all identifiable risks (Levi and Wall 2004). An identifiable risk could be of a politicised-military, economic, societal or environmental character but framed as a security problem as a systematic approach to counter its potential threat (Buzan et al. 1998). Given the emphasis on the socially constructed form of securitisation, of mainly pertaining to societies rather than individuals, governments have started to introduce exceptional measures, usually beyond the common frequently used and established rules of the political system, brought into practice as an absolute necessity to maintain the security of the society and its interdependent critical infrastructures (Cavelty 2007).

At the same time, however, governments' accession to the newly unprecedented powers have risen true concerns from the public, to the extent that many people started to perceive the processes as gradual introduction of blanket overt/covert policing on many aspects of the human life, ultimately leading the way to a "total surveillance society" (Garfinkel 2000; Rule 2007). The "Ring of Steel" security initiatives both in Central London, the UK, and in Lower Manhattan, New York City, the United States, are arguably good examples. These initiatives are basically networks of extensive closed-circuit television (CCTV) systems that provide law enforcements and security personnel with 24/7/365 visibility of vast number of areas, roads and facilities. Although these systems turned to be somewhat useful, such as occurred in detecting suspicious behaviours in the 2004 Madrid train bombings in Spain, and enabling the identification of several terrorists in the 2008 Mumbai, India attacks, a direct result of the their omnipresence is that a person should expect to be recorded, in real time, several times a day without a need to get a prior consent or demonstrate any probable reason to that person. Contrary to what is expected, these technologies have led to a noticeable shift of insecurity amongst people, ultimately

introducing genuine concerns of possible privacy infringements (Sahm 2006).

In the anticipated national emergency warning system in Australia, the system should basically allow the government, primarily under emergency declarations, to be able to determine the almost exact geo-location of all active cellular handsets in a pre-defined threatened area(s), or track mobile phones in real time within designated risky zone(s), and then disseminate, and re-disseminate when necessary, a blanket waring message to these mobile phones.

Receiving the message does not necessarily require an explicit consent from the recipient since pertinent government departments and law enforcement agencies have the power, under the current applied Privacy Act 1988, to temporarily waive the person's right to privacy in the emergency situation based on the assumption that the consent is already implied when collecting locational information in such situation.

Emergencies do represent unique contexts where privacy is most likely to be one of our least concerns. In theory, the determination/tracking processes must not trigger any privacy issues when being specifically utilised for emergency purposes. The problem does not stem, however, from this specific utilisation but from the general perception of the uninterrupted availability of the determination/tracking technologies, being in the hand of the government during normal daily life activities. This perception has the potential to raise acute concerns. Locational information could be collected, stored, aggregated, and when correlated with other personal information, a broad overview of behavioural patterns or detailed portraits of individual habits could be created (Parenti 2003; Clarke and Wigan 2008). Indeed, this profiling of individuals is what makes people uneasy, because of concerns about privacy in general as well as fear of being incorrectly labelled (Holtzman 2006).

Without discarding the apparent fact that the system has the potential to save lives, shutting down the "flows of information" as a react to any concerns sounds completely unrealistic thinking in the "transparent society" of today, especially, when sharing information is perceived as mutually beneficial in such circumstances (Brin 1998). Nonetheless, there is a need to find a balance between the individual's right to privacy and the government's call for exploiting location-based emergency services, as the next essential step towards the securitisation of today's society. The privacy-security telecommunications deadlock may occur when a person is faced with the dilemma of how much personal identifiable information he or she is willing to ceaselessly relinquish in exchange of a continuous secure society?

The next section of this paper provides a general overview of location-based services and their utilisation as a means of security. Section 3 discusses the reasons that would arguably trigger concerns from utilising the emergency warning system under emergency declarations, hence, initiating a possible privacy-security telecommunications deadlock. Section 4 provides general directions and suggestions formed to partially aid resolving the expected deadlock. Section 5 concludes the paper.

2 Location-based Services as a Means of Security

Location-based services (LBS) utilise the collected geo-locational information of the target cellular mobile phone in order to add value to the provided service. The location information could be stored for the purpose of further processing or it could be combined with other pertinent information and then sent back to the user in a value-added form such as a nearby point of interest or navigational directions. The location information may be obtained by using various positioning techniques that differ in their cost, coverage and precision. In general, the accuracy of the positioning results usually ranges between a few meters up to several kilometres. The received service could take the form of a bitmapped image or a message (text, voice, or multimedia). The user could either initiate a request for the service or the service could be triggered when the handset enters, leaves or comes in the vicinity of a pre-defined zone (Küpper 2005).

In emergency situations, LBS have been traditionally utilised to find the almost pinpoint geographic location of a person after he or she initiated a distress mobile phone call or a short message service (SMS) request for help. Another complement, but relatively new, utilisation of LBS involves the dissemination of rapid public alerts, warning messages or relevant safety information from relevant government agencies, in collaboration with the telecommunication carriers and mobile phone service providers, to all active handsets within a designated area(s) regarding a security issue if it happened or was about to happen in the vicinity of the active handsets (Aloudat et al. 2007).

The utilisation of LBS under a national emergency warning system has the advantages of enabling in and out zone reporting and messaging/re-messaging to a mass number of people (Kidd et al. 2008), providing an effective solution to aid in the creation of control zones for almost every imaginable threatening scenario. See Figure 1 for an example. LBS could be utilised to target the population in the unsafe zone or its surrounding zones, in almost real time dissemination of safety information, before, during or in the aftermath of the event, specifically targeting those who are not anchored at the time to a TV, radio, internet or any other informative channel. The services have the potential to augment the levels of security by increasing the situational awareness amongst the recipients of the waring message about a specific threatening event, thus helping to avoid further casualties or damages.

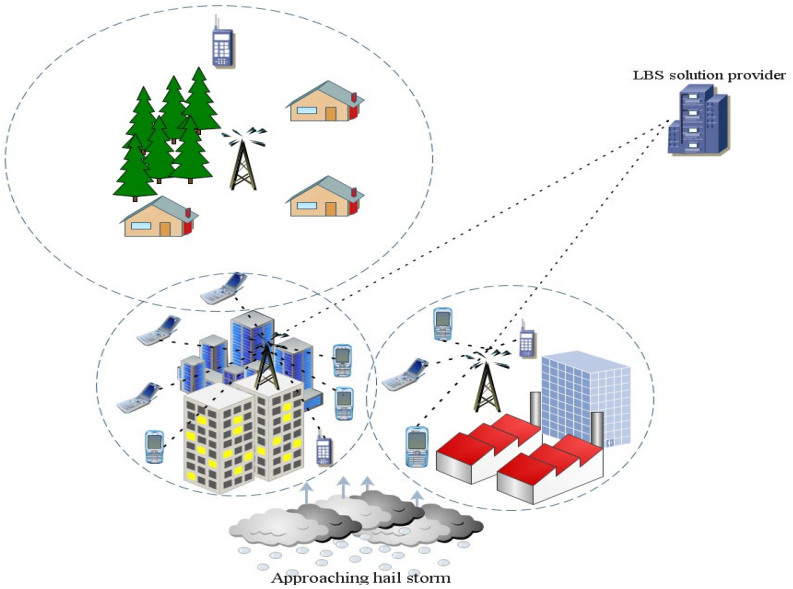


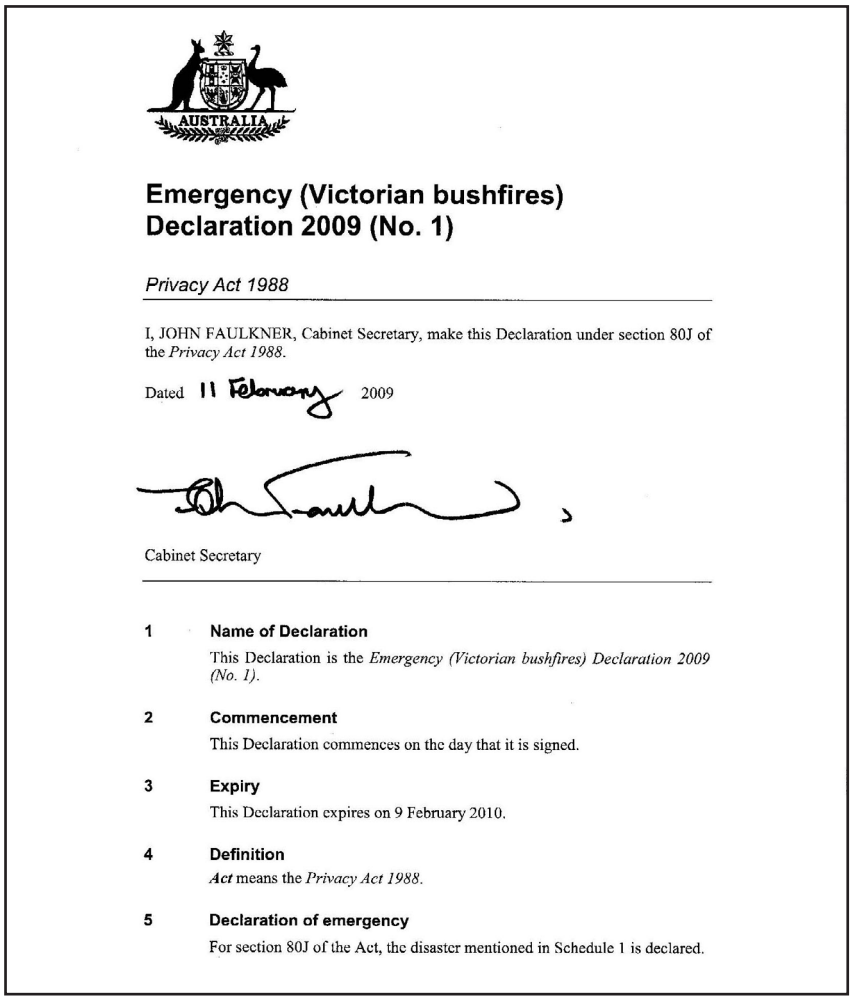
Figure 1: An example of delivering a blanket information message service about an impending hazard based upon the geo-location of the active handset

3 Privacy-Security Deadlock Under Emergency Declarations

On February 11th 2009, the Honourable Senator John Faulkner, a Cabinet Secretary and Special Minister of the State, signed the Emergency Bushfires Declaration No.1 on behalf of the Victorian Government while Victoria was experiencing one of its worst natural disasters in its recorded History.The declaration was made under Section 80J of the Privacy Act 1988. See Figure 2.

Section 80J is primarily concerned with the declaration of an emergency or an event of a national significance and only the Prime Minister of Australia or the Minister of relevance may make such a declaration, as the case may be, if:

1. An emergency or disaster has occurred; and
2. The emergency or disaster is of such a kind that it is appropriate in the circumstances for this part to apply in relation to the emergency or disaster; and
3. The emergency or disaster is of national significance, whether because of the nature and extent of the emergency or disaster, the direct or indirect effect of the emergency or disaster, or for any other reason; and
4. The emergency or disaster has affected one or more Australian citizens or permanent residents, whether within Australia or overseas.



Emergency (Victorian bushfires) Declaration 2009 (No. 1)

Privacy Act 1988

I, JOHN FAULKNER, Cabinet Secretary, make this Declaration under section 80J of the *Privacy Act 1988*.

Dated 11 February 2009

Cabinet Secretary

1 **Name of Declaration**

This Declaration is the *Emergency (Victorian bushfires) Declaration 2009 (No. 1)*.

2 **Commencement**

This Declaration commences on the day that it is signed.

3 **Expiry**

This Declaration expires on 9 February 2010.

4 **Definition**

Act means the *Privacy Act 1988*.

5 **Declaration of emergency**

For section 80J of the Act, the disaster mentioned in Schedule 1 is declared.

Figure 2: The emergency bushfires declaration

Because of the extent of damage and loss in Victoria, which require a lot of time for recovery and restoration and also the prudential need to prepare Victorians who could be in the affected reach of the next bushfire season the declaration has been set to expire after almost one year from its commencement date.

On March 2nd 2009, under the declaration, more than 3 million mobile phone users, resided at the time in threatened bushfire areas in Victoria State, received SMS messages warning them of the extreme weather conditions expected the next day. Telstra, Optus and 3 Hutchison, the three main mobile phone service providers in Australia, sent an identical message to their customers on behalf of the Victorian Emergency Services (Dobbin 2009).

The Privacy Act, under the National Privacy Principles (NPP) Subclause 1.3, explicitly indicates that the Australian individual has the right to know: (i) who is collecting personal information about him or her, (ii) the purpose of the collection and, (iii) what happens to the information after it has been collected. The NPP

however made a notable exception to these rules in emergency situations, when the possibility of a serious threat to the life or the health of the individual is high, as it may not be reasonable to take the aforesaid awareness steps in such circumstances. The Act defines *personal information* as " information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" (Australian Government: Attorney General's Department 2008). The Act does not define exactly what type of personal information would be collected during emergencies, but under the broad understanding of the definition, any identifiable information is personal information, including the locational information of the mobile phone user.

In the case of an emergency, every mobile service provider in Australia is committed to provide the Integrated Public Number Database (IPND), law enforcement agencies or the regulatory authorities with any requested personal information it may have on its customer, including the locational information of the individual's mobile phone. This is explicitly defined in every provider's privacy policy, which the user agreed upon once started his or her mobile phone service. However, it should be noted that almost all privacy policies do not indicate whether or not the individual would be informed or made aware about the type of information that would be collected, stored or passed to other parties in the case of an emergency.

The mentioned issues may not be foreseen to raise any privacy concerns when an emergency is unfolding or taking its tolls. However, in order to determine whether or not there is a need to make a decision to send a warning message to a specific mobile phone the emergency warning system should be able to keep tracking the whereabouts of the phone to identify the contiguous proximity of its last known location to the potential risk. A considerable space for genuine concerns may originate here since, being under a one year long emergency declaration, the Australian individual may never know the extent of tracking or the breadth of information being collected and passed upon request from his or her mobile service provider to the government. Although could be merely misconceptions, but the idea of the government's ability to extract behavioural patterns or create detailed profiles about individuals from the attainable information, may widely open the door for a possible privacy-security telecommunication deadlock if not treated properly under future emergency declarations.

4 Avoiding the Deadlock

With the additional security measures that go beyond the traditional four phases of emergency management (i.e. preparedness, response, mitigation and recover), infringements to some privacy rights are quite possible to occur. Accordingly, the polarity between security and privacy could be augmented to the extreme opposite in the eyes of the public if both issues are not considered or treated carefully. There

is a need to early avoid a possible privacy-security telecommunications deadlock by start engaging the public in the securitisation processes underlying the deployment of the national emergency warning system. The following presents some of the suggestions to be taken in this regard:

4.1 Towards the Risk Society

Templeman and Bergin (2008) argued that there have not been any adequate effort to prepare Australians on how to manage and cope with the high consequences of large-scale emergencies and disasters, for example, Australia still has not "conducted a public communications campaign to inform householders on how they could cope if a human influenza pandemic occurred". While the 2009 H1N1 virus flu pandemic is strongly presented as a worldwide threat today, Templeman and Bergin (2008) asserted that Australia does not met the minimum disaster preparedness standards, specifically in the health system, where the Australian hospitals are way below the preparedness benchmarks set by United States hospitals for mass casualty incidents. In addition, Bergin (2008) expressed his doubt of the ability of the Australian different governments to "deal with a population that, in the main, has little experience of such serious sudden events".

This lack of preparedness from the government and also from the public is fairly due to a long shared belief that large-scale disasters in Australia are rare and the occurrence of one will always be a highly distinct possibility. This belief has significantly lessened the general perception of the seriousness of the extreme events and would always influence negatively on people's acceptance to any additional security measures. Accordingly, there is a need to continually engage the public to recognise the diversity of risks facing Australia. Engaging them would help building up a constant serious-minded state towards emergencies and ease the transformation of the Australian society into a risk society; a society that is prepared and organised enough to absorb the potential effects of all types of hazards, ranging from manufactured risks, as the product of human inadvertent or deliberate activities, to the risks of natural events. It is strongly argued that the risk society has more ability to understand, accept and adapt to any additional security measures, hence alleviating any extreme concerns toward privacy issues.

4.2 Create a Knowledgeable Society

As mentioned earlier, the utilisation of the system under emergency declarations could be dimmed by misconceptions about the uninterrupted availability of its underlying tracking technologies, being used for instance to profile individuals' whereabouts in times and places beyond emergencies. Without clearing such misconceptions, it is reasonable to postulate that concerns about privacy would always originate.

It is noted, however, that no educational campaigns have been conducted by the government to increase awareness regarding the deployed system, and in a way that

could help clearing these misconceptions. As an ultimate purpose for the system's utilisation is to help saving lives, it should be then in the government's best interest to provide the public with the adequate level of information about its benefits, its underlying technologies and its limitations. The government should also express its legal and ethical obligation to protect the confidentiality of the accessed locational information. Such fundamental knowledge and understanding could offer the kind of assurance that has the ability to alleviate the concerns while, at the same time, help in the development of a general appreciation for the practiced security measures.

5 Conclusion

Emergencies are security challenges that have the potential to disrupt the orderly way of today's civil society. While there is a growing trend from governments to deploy more socially constructed security measures to counter the threatening consequences of these extreme events, the public reception has not been always in the favour of such deployment, where many people perceived these measures as a start to a gradual relinquish of their privacy rights.

This paper discussed the possibility of a privacy-security telecommunications deadlock, which could emerge under the new national emergency warning system in Australia. Particularly, when the anticipated location-based identification of the active mobile phones for emergency notification purposes is deployed under the system. The paper presented the concerns that may originate from the public perception of the continuos availability of the system's tracking technologies, being utilised during a one year long emergency declaration in times and places beyond the emergency itself. Although these tracking mechanisms are strictly bounded by laws and privacy acts with an explicit restricted utilisation to be for emergency purposes only, it is argued that most of the common people do not have such kind of knowledge. With no true effort from the government to raise the awareness about the deployed system, most of the concerns, although may merely be misconceptions, have the power to impact negatively on the practiced security measures while devaluing the purpose of system in the eyes of the public.

The paper stressed the need to increase the public appreciation for the system by augmenting the perception of the seriousness of emergencies facing Australia. In addition, the paper emphasised the need to change the mindsets of the people about the government's sole responsibility in managing emergencies. This could be done by positioning the Australians at the centre of this societal system through extensive educational and preparedness campaigns, transforming them into an active partner instead of a mere passive recipient. A risk and knowledgeable society would likely to have more ability to discern that security is a shared responsibility each individual has to endure for the sake of a safer way of life for everyone.

References

Aloudat, A., Michael, K. & Jun, Y. 2007, 'Location-Based Services in Emergency Management- from Government to Citizens: Global Case Studies', in P. Mendis, J. Lai, E. Dawson & H. Abbass (eds), Recent Advances in Security Technology, Australian Homeland Security Research Centre, Melbourne, pp. 190-201.

Australian Government: Attorney General's Department 2008, Privacy Act 1988: Act No.119 of 1988 as amended, the Office of Legislative Drafting and Publishing, viewed 02 August 2008 <http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/63C00ADD09B982ECCA257490002B9D57/$file/Privacy1988_WD02HYP.pdf>.

Bergin, A. 2008, 'There's a storm bigger than terrorism and only we can save ourselves', The Sydney Morning Herald, September 4, 2008, viewed September 14, 2008 <http://www.smh.com.au/news/opinion/theres-a-storm-bigger-than-terrorism-and-only-we-can-saveourselves/2008/09/03/1220121326178.html>.

Brin, D. 1998, The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?, 1st edition, Perseus Press, Boulder, Colorado.

Buzan, B., Wver, O. & Wilde, J.D. 1998, Security: A New Framework for Analysis, 1st edition, Lynne Rienner Publishers, London.

Cavelty, M.D. 2007, 'Cyber-Terror–Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Journal of Information Technology & Politics, vol. 4, no. 1.

Clarke, R. & Wigan, M. 2008, 'You are where you have been', in K. Michael & M.G. Michael (eds), Australia and the New Technologies: Evidence Based Policy in Public Administration, University of Wollongong, Canberra, pp. 100-114.

Dobbin, M. 2009, 'Victorians Receive Fire Text Warning', The Age, March 3, 2009, <http://www.theage.com.au/national/victorians-receive-fire-text-warning-20090302-8mfq.html>.

Garfinkel, S. 2000, Database Nation: The Death of Privacy in the 21st Century, 1st edition, O'Reilly & Associates, Inc., Sebastopol, California.

Holtzman, D.H. 2006, Privacy Lost: How Technology Is Endangering Your Privacy, 1st edition, Jossey-Bass, San Francisco, California.

Kidd, A., Loasby, K., Treadgold, G., Hoskin, K., Chong, K. & Caldwell, S. 2008, New Zealand Telecommunications Based Public Alerting Systems Technology Study, New Zealand Centre for Advanced Engineering, University of Canterbury Campus, Ministry of Civil Defence & Emergency Management, Christchurch, New Zealand, viewed 12 August 2009, <http://www.mcdem.govt.nz/memwebsite.nsf/Files/Public-alerting/$file/CAENZ-Report.pdf>.

Küpper, A. 2005, Location-Based Services: Fundamentals and Operation, 1st edition, John Wiley & Sons Ltd., Chichester, West Sussex.

Levi, M. & Wall, D.S. 2004, 'Technologies, Security, and Privacy in the Post-9/11 European Information Society', Journal of Law and Society, vol. 31, no. 2, pp. 194-220.

Parenti, C. 2003, The Soft Cage: Surveillance in America From Slavery to the War on Terror, 1st edition, Basic Books, New York.

Rule, J.B. 2007, Privacy in Peril: How We are Sacrificing a Fundamental Right in Exchange for Security and Convenience, 1st edition, Oxford University Press, Inc., New York.

Sahm, C. 2006, Hard Won Lessons: Transit Security, Safe Cities Project, Manhattan Institute, New York, <http://www.centerforpolicingterrorism.net/pdf/scr_05.pdf>.

Templeman, D. & Bergin, A. 2008, Taking a Punch: Building a More Resilient Australia, The Australian Strategic Policy Institute, viewed 02 February 2009, <http://www.aspi.org.au/publications/publication_details.aspx?ContentID=165>.

10

Demonstrating the Potential for Covert Policing in the Community: Five Stakeholder Scenarios

Roba Abbas, Katina Michael and MG Michael
University of Wollongong

Abstract

This paper presents the real possibility that commercial mobile tracking and monitoring solutions will become widely adopted for the practice of non traditional covert policing within a community setting, resulting in community members engaging in covert policing of family, friends, or acquaintances. This paper investigates five stakeholder relationships using scenarios to demonstrate the potential socio-ethical implications that tracking and monitoring people will have on society at large. The five stakeholder types explored in this paper include: (i) husband-wife (partner-partner), (ii) parent-child, (iii) employer-employee, (iv) friend-friend, and (v) stranger-stranger. Mobile technologies such as mobile camera phones, global positioning system data loggers, spatial street databases, radio-frequency identification and other pervasive computing, can be used to gather real-time, detailed evidence for or against a given position. However, there are currently limited laws and ethical guidelines for members of the community to follow when it comes to what is or is not permitted when using unobtrusive technologies to capture multimedia, and other data that can be electronically chronicled. The evident risks associated with such practices are explored.

Keywords: community policing, covert policing, scenarios, GPS, LBS, socio-ethical

1 Introduction

The availability, prevalence and proliferation of mobile tracking and monitoring solutions enable community members to independently gather location data for their own needs. In the market today are commercially available devices and technologies such as GPS data loggers, spatial street databases, mobile camera phones, and radio frequency identification (RFID) tags, which facilitate the collection and capture of data related to the location of an individual. The information gathered from these devices can potentially be viewed in real-time, and may relate to habits, behaviours and trends. Furthermore, the devices support the compilation, display and manipulation of the location data, resulting in improved processing capabilities, and the application of the data and devices in novel situations, such as covert policing within a community setting. That is, technologies that were once considered components of professional policing and law enforcement strategies have deviated from the policing realm, and are now available to community members. Effectively, this grants individuals complete power in conducting independent, covert policing activities within their social network. However, these practices lack the professionalism, checks and constraints afforded in the more conventional forms of (community) policing, thereby introducing socio-ethical consequences. This paper introduces and demonstrates the potential for covert policing in the community through a set of socio-ethical scenarios, which enable the ensuing implications of covert policing within the community to be investigated.

2 Method

This paper explores the potential for covert policing within the community by way of concise but demonstrative scenarios, which are supplemented by related literature, in order to draw out the emergent socio-ethical dilemmas. Scenarios have confirmed their value in previous studies regarding location-based and mobile tracking technologies to allow for an evaluation of the future social impacts of emerging technologies (Perusco and Michael, 2006) and to establish the need for privacy controls for location technologies (Myles et. al., 2003), rendering them a fitting explanatory tool for the purposes of this paper.

The scenarios developed below are based primarily on a societal relationships taxonomy, which defines the main social interactions or relationships amongst community members. The societal relationships taxonomy is modelled on categories utilised in a recent study and report titled "The Next Digital Divide: Online Social Network Privacy", which focuses on the use of online social networks (ONS) by young Canadians, and by organisations for commercial purposes (Levin et al., 2008). Importantly, the study evaluates the user's perception of risk and privacy protection in using OSN, requesting that respondents indicate their concern about who is granted access to their online information. The response categories provided are: (i) friends, (ii) parents, (iii) other family member, (iv) employer, and (v) people you don't know (Levin et al., 2008).

These categories have been adapted to form the societal relationships taxonomy for this paper, as they offer a representation of the major social relationships that exist, and therefore offer guidance and a comprehensive approach to developing the socio-ethical scenarios. However, while the aforementioned study is centred on perceptions of risk and additional concerns in an online setting, this research deals with each of the stakeholder categories in a physical setting and thus the categories have been modified to focus on the distinct physical interactions or relationships that may exist in a community social network. The five stakeholder types explored in this paper include: (i) husband-wife (partner-partner), (ii) parent-child, (iii) employer-employee, (iv) friend-friend, and (v) stranger-stranger. Each of these stakeholder types is represented by a demonstrative scenario, which is constructed and explained using existing studies and literature. Figure 1 identifies the systematic process adopted throughout this paper, displaying the relationship between the societal relationships taxonomy, literature and scenarios.

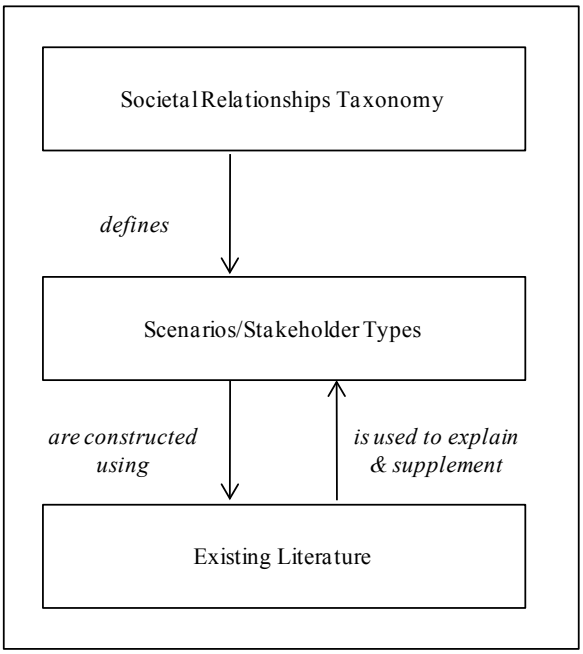


Figure 1: Process and method used throughout this paper

3 Scenarios

This section discusses the stakeholder scenarios, initially offering the concise scenario followed by a discussion of the socio-ethical consequences of covert policing in the community.

3.1 Husband-wife (partner-partner)

Scenario: Ted Johnson had arrived home late from work five days in a row, and had not been himself for some time. After repeated attempts to find out what was

wrong his wife, Jenny, was fed up with Ted's claims that he was overloaded at work. After all, this was the first time in 17 years that Ted had worked overtime. Having heard about a new GPS logging device that was available for some three hundred dollars, Jenny placed the device in Ted's car, behind the tissue box next to the back window where he was unlikely to notice the somewhat hefty unit. What if Ted had been lying to her? Jenny could not wait to confront him with details of his location if this was to happen again. She was convinced he had something to hide; now she would have proof…

Developments in mobile monitoring and tracking technologies are enabling a shift from use by law enforcement/policing agencies to general members of the public. While noting the positive applications of such technologies for law enforcement and other situations, a number of concerns must be addressed. That is, technologies are now available commercially, require little knowledge of the technical aspects to operate, and can be used for purposes such as spousal tracking (Dobson, 2009). Spousal tracking can be considered a form of 'Geoslavery', which Dobson and Fisher (2003) describe as the ability to monitor and control the physical location of an entity, effectively empowering the 'master' who controls the other entity or entities (the 'slave').

When discussing the husband-wife scenario, a multitude of products, such as commercially available GPS tools and digital cameras/mobile phones (providing still and video footage) can be used to track the whereabouts of a partner, essentially diminishing the amount of control the victim or 'slave' possesses. Furthermore, an individual can gather evidence for or against a particular case, as implied in the provided scenario through the concept of 'proof', and can confirm the findings through multiple means/technologies. An immediate danger that can be observed in this scenario or broadly in the tracking of family members is the threat of technology abuse, and the potential to encourage suspicion and importantly distrust (Barreras & Mathur, 2007). In an article that describes the uses and privacy concerns pertaining to wireless location-based services, it is argued that "The very act of monitoring destroys trust, implies that one cannot be trusted" (Michael in Ferenczi, 2009: 101). This notion is an underlying theme within the scenario, as Jenny is convinced that her husband is concealing his whereabouts, jumping to the conclusion that be may be lying, and thereby questioning Ted's trustworthiness.

Apart from the potential for misuse and the trust-related implications, privacy is an imminent concern when spousal tracking takes place. Individuals tend to lobby for increased privacy where institutional surveillance and monitoring activities take place, but are less wary of such activities being employed by families, notably within parent-child and spousal/husband-wife relationships (Mayer, 2003). Technologies such as internet tracking, GPS, miniature cameras and genetic tests are intended to be used to increase levels of safety for individuals within a family unit; however, Mayer (2003) believes that this can be damaging in terms of privacy, safety, and may also affect trust between family members.

In the husband-wife scenario, one must raise concern over the potentially damaging results of selective and continuous monitoring of partners. In selective situations, there is the danger of incriminating a spouse based on an incomplete picture or details. Continuous monitoring activities, which involve 24/7 monitoring and two-way communication (Dobson, 2009), run the risk of high degrees of surveillance and excessive levels of distrust, which is an unhealthy outcome. Moreover, data that has been collected using GPS-enabled devices is not always accurate and can be manipulated to provide information that conflicts with reality (Iqbal & Lim, 2008), a highly relevant consideration in the husband-wife and remaining stakeholder scenarios. This scenario encourages a number of questions: In using covert policing in a spousal situation, what are the relationship-related consequences? How will technological inaccuracies be factored into the decisions made based on the collected data? Will a partner take the law into their own hands? What actions are triggered by the assumptions made by the partner? How serious are the repercussions, for instance, physical violence or divorce?

3.2 Parent-child

> *Scenario: The past week had been a trying one for the residents of a regional town in New South Wales, Australia. Word had spread of a near-kidnapping close to the public school, and the Kumar family were concerned about their eleven year old son's safety, as he had to walk home alone from school, given the current situation at home and the need for mum, Rachna, to be at work. Rachna felt that if only she was able to monitor her son unawares until he had reached home, she would have peace of mind that he was ok and not have to rely solely on his promise that he would go home directly after school. A few Internet searches later, she had found the answer. All Rachna had to do was subscribe monthly, place the GPS-enabled device in her sons backpack, and access the secure website while at work. Simple! The investment would be worth the safety of her child…*

The convenience associated with GPS monitoring and tracking technologies simplifies the ease with which such technologies can be used by family members, particularly in the parent-child scenario. That is, GPS technologies come in the form of handheld, wearable and embedded devices, may be used to track the whereabouts of children such as the Wherifone wireless device (Michael et al., 2006) and the Verizon Wireless Chaperone (Ferenczi, 209), and can be deployed in many different ways, both overtly and covertly. Generally, parent-child solutions are promoted as being technologies that increase safety levels. For example, Barreras and Mathur (2007) review family tracking software that is intended to provide knowledge of the location of family members, in order to maintain and provide protection. The solution is primarily attractive to parents who wish to monitor their child's movements, relying on continuous updates and the presentation of information on a secure website, as was the case in the above scenario. There is the perception that the solutions will ensure children are accountable for their behaviour, and some

view the technology as aiding and enhancing traditional parenting tasks.

The benefits of GPS technologies in the parent-child scenario are therefore specifically evident in two situations, which include the protection of young children who travel unescorted, and also the monitoring of young adults using commercial and portable systems that are fairly inexpensive to implement and are rather discrete in physical characteristics (Mayer, 2003). This makes GPS and monitoring technologies ideal for covert uses, as commercially attainable GPS devices come in a number of forms, varying in size, capacity and complexity. These devices can be carried and worn in overt scenarios, and be placed amongst personal items within bags or obscured from view within a vehicle, making the device virtually undetectable. However, in the parent-child situation, the integrity of the solutions is questioned, given that children can remove or ask a friend to carry the device.

While such technologies have been used by law enforcement agencies for some time, it should be mentioned that the commercial alternatives do not require a high level of technical sophistication to implement. However, what are the resulting affects on trust, privacy and family relationships in general?

A study on parental monitoring and trust maintains that a parent's trust in their child develops based on three types of knowledge: concerns/feelings which are linked to the beliefs or values a child possesses; information concerning past violations; and knowledge of a child's daily activities in varying situations which is linked to responsibility and judgement (Kerr et al., 1999). Importantly, the latter is weighted as an important form of knowledge, and information can be elicited in a number of ways.

The information can be provided freely by the child, the parent can prompt the child for knowledge, or alternatively parental control techniques can be adopted where specific rules are imposed on the child. With the introduction of commercially attainable GPS technologies, the provided scenario proposes that a fourth method can be utilised to obtain knowledge of a child; that is, the use of commercial technologies implemented covertly. However, a major concern that emerges from this form of knowledge elicitation is: what contribution/impediment will this make to (a) parental trust, and (b) the trust a child has in their parent?

Applying these claims to covert tracking in the parent-child scenario, one can immediately pinpoint concerns regarding the covert tracking of children, particularly in view of trust. For instance, why did Rachna feel the need to use a device covertly, rather than rely on her son's account? Could she have been more transparent regarding her safety concerns? What would ensue if the child was to discover he was being tracked? Furthermore, what impact would excessive tracking have on the development of the child? Is child tracking eroding the idea of private space, and thus prohibiting children from developing fundamental skills? Michael and Michael (2009) build on this notion of private space, in an article that discusses the privacy implications of 'Überveillance', which is considered, at the fundamental level, "an exaggerated, and omnipresent 24/7 electronic surveillance" (p. 86). The authors

highlight the importance of being granted a private 'location' or space in which to flourish, develop and discover one's identity free from continual monitoring. With regards to the parent-child scenario, it is apparent that tracking technology may prohibit children from learning or developing 'street smartness' and other vital skills. Therefore, in an attempt to protect their child from 'society', parents can simultaneously be impeding the child's development, and the manner in which they view the role of trust (amongst other things) in relationships.

When considering the parent's position, it is important to note that their perception of their child and the associated level of trust they have would also be affected/alter in the process of practicing independent policing activities. While from the parent's perspective, the attainment of knowledge contributes to a trusting relationship, Kerr et al. (1999) found that the source of such knowledge in an essential factor. That is, the spontaneous disclosure of daily activities is favourable to other sources of knowledge gathering, and correlates to higher levels of trust on the part of the parents. In gathering knowledge, family members often utilise monitoring and tracking technologies in the interest of the safety of their loved ones and with the best intentions, but this is generally conducted without consideration of the damaging nature of such activities, relinquishing trust and privacy in the process (Mayer, 2003). Similar articles review the use of child trackers to allow parents to identify the location of their child on a map or request the location of their child at any given time, also flagging the related privacy and trust issues (Schreiner, 2007).

In the context of covert policing within a community setting, a number of questions are pertinent. What consequences arise when a parent has knowledge of the daily activities of their child (for both parties)? How will GPS and other forms of technologies perform as a valid knowledge gathering source? Will the technologies contribute to or impede trust in parent-child relationships? Have the child's rights been considered? What will be the long term affects of parental monitoring and the covert policing of children? Does the use of parental monitoring solutions encourage a false sense of security for parents, particularly given the risk of a criminal 'breaking' into or compromising the tracking system?

3.3 Employer-employee

> *Scenario: Called into his manager's office, Tom slowly closed the door behind him. It was unlike Ms Sanders to call one-on-one meetings with her staff, particularly members of the Delivery Team; this made Tom a little nervous. He had not been in a conflict with anyone and was generally happy with his occupation. "Tom it has come to my attention that you have been in breach of your contract. I regret to inform you that we will have to let you go…"*

Emerging technologies facilitate not only the collection of employee data, but the storage and processing of such information, raising apprehension over information being used for purposes other than the intended (Levin et al., 2006). A primary example is the use of unobtrusive GPS devices for covert policing applications.

In this situation, an employer may utilise employee location details to incriminate individuals or to 'police' the activities of their subordinate in an unauthorised fashion, which was the case in Tom's situation above. The implications of employee monitoring in general are discussed in numerous studies, a selection of which are offered below, providing insight into the related risks.

Chen and Ross (2007) discuss the concept of electronic workplace monitoring, including the tracking of Internet usage and email communications. Specifically, their study focuses on variations in individuals' personalities and demographic factors which affect the manner in which individuals respond to being monitored at work. The research discusses the use of electronic performance monitoring technologies, including GPS for vehicle location tracking, presenting both the positive and negative consequences that may result from such activities, while introducing a framework for evaluating individual differences in order to predict reactions to being monitored. In reviewing the literature, Chen and Ross (2007) identify gains such as reduced crime, enhanced customer relationships and productivity improvements. Similarly, the risks are articulated and include negative behavioural impacts, attitudinal effects and ethical concerns.

Other scholars elaborate on such perspectives, and offer additional examination of the risks associated with unwarranted levels of employee monitoring. Kaupins and Minch (2005) focus on the use of emerging technologies to monitor the location of individuals in a workplace setting, focussing on GPS solutions (outdoor, broader scale) through to sensor networks (indoor). The authors also point to the legal and ethical implications of having Internet/email communications and general work behaviours monitored by employees, citing security, productivity/performance enhancements, reputation and enhanced protection of third parties as being the encouraging facets of employee monitoring. Kaupins and Minch's (2005) inverse argument examines privacy, accuracy and inconsistency as being significant concerns of monitoring practices, with privacy also being cited by Townsend and Bennett (2003) as a chief concern, inevitably resulting in an undesirable work atmosphere between employer and employee. Weckert (2000) also reports on trust-related issues emerging from excessive monitoring of employees, contributing to deterioration in professional work relationships.

While the above discussion has focussed on the implications of monitoring from an employee perspective, some studies examine employer attitudes regarding the workplace privacy and monitoring/surveillance debate. For instance, Levin et al's (2006) study revealed that while employers admitted to using monitoring and surveillance techniques for benefits such as safety and security, fleet management, and employee training and development, they did not actively exploit the secondary uses of the monitoring technologies. With respect to the use of GPS technologies, the interviewed employers considered GPS technologies as a supply chain and fleet management solution first and foremost. Devices such as commercial mobility solutions (including GPS devices and in-car units), digital cameras and mobile

phones, and electronic tags collect adequate information about an employee which can be used to promote efficient work practices and accountability, whilst providing employers with real-time access to information. However, this does not eliminate the fact the GPS technologies can be used for secondary purposes, and moreover in a covert manner, particularly in cases where employers obtain a work phone without realising they can be tracked.

The implications of employee monitoring have been briefly identified; it is therefore imperative at this point to consider the covert angle with respect to the supplied scenario. Deceptive or concealed monitoring and tracking may result in trust being diminished in professional relationships, even in situations where high levels of trust exist. This is due to the fact that location information is often assured as accurate, despite the potential for inaccuracies to exist regarding the whereabouts of an employee. For instance, in deconstructing the employer-employee scenario, Ms Sanders did not question the source and validity of her information, in that she was not open with respect to how she came in possession of details to prove Tom was in 'breach' of his contract. Rather, she opted to 'police' the situation immediately, concluding that her employee was 'guilty' of requesting remuneration for work he could not have completed, according to the location data.

Concerns inevitably escalate when covert means of tracking are present, based on the premise that secret or deceptive monitoring will affect open transparent relationships, affecting employer-employee relationships. This notion is alluded to by Herbert (2006) in paper which examines the legal issues associated with human tracking technologies such as GPS, RFID, cellular technology and biometric systems. The author claims that tracking technologies enhance the power and control given to employers, and therefore secrecy is required to avoid employee backlash with respect to the installation of monitoring systems. Herbert further asserts that such systems allow employers to monitor not only work-related activities, but also personal data and habits, which can be compromised and result in subordinates seeking legal protection, and in essence rebelling against their employers. Therefore, it appears that there is the need for a more transparent approach. For example, Kaupins and Minch (2005) suggest the introduction of policy manuals and employee handbooks when implementing employee monitoring in the workplace. Other regulatory and policy issues need to be explored, and a practical and actionable solution be proposed, one which protects the interest of both stakeholders in the employer-employee scenario. The primary question posed is: How do employers reconcile the opposing ideas of protecting personal privacy with encouraging productive and efficient behaviours/attitudes in the workplace?

3.4 Friend-friend

Scenario: This year, university friends Anna and Chris had been competing heatedly with one another to find out who could play the best practical joke. Having received a 'cool' GPS monitoring device for a class assignment about new

innovations in IT, Anna thought it would be great to track Chris and show him that she knows where he has been, just like Big Brother! Step one was to conceal the device without Chris knowing. This was easier than Anna had anticipated given how close they were. Recovering the device two days later, Anna could not wait to show Chris. Looking at the first three hours worth of data, she just had to laugh. Chris was so predictable! Looking on, Anna noticed Chris had not travelled to Sydney on Wednesday, as he had mentioned. Why did he tell her that he would be away all day?

The previous scenarios have alluded that emerging technologies are moving beyond government-related (and policing) applications, and are being applied in more family, friend and employee-centric applications (Barreras & Mathur, 2007). The friend-friend scenario will further build on the identified risks and implications.

Prior to engaging in a discussion of risks, it is necessary to point out the alternative and positive argument that such technologies may have. If used in an overt manner, GPS monitoring devices can offer convenience in planning social events, and may in reality provide built-in safety and privacy features from a technical standpoint. As such, several GPS-based solutions and location technology vendors promote the safety angle in friend-friend scenarios, maintaining that privacy and safety are in fact enhanced, in that friends have power over who can access their location and assist in emergency or undesirable situations respectively (Schreiner, 2007).

The friend-friend scenario, however, provides an alternative viewpoint with less desirable connotations. This scenario questions the amount of control individuals possess over their location data, specifically, who holds access to their location information. A valuable comparison is to evaluate similar concerns within the online social networking space, where individuals are able to select their 'friends' and define the level of access granted to them on an individual basis. This form of control is diminished in the friend-friend scenario; for instance, Anna was able to independently track Chris' location, while Chris was seemingly unaware and did not have the power to restrict such activities, as it was not a two-way agreement.

Given the covert nature of such activities, concerns regarding control are significantly enhanced, as covert policing in the friend-friend scenario prohibits individuals from retaining the right to limit access to their details. The detrimental outcome of this situation is a loss of privacy.

In a related study on privacy and location-based services, Myles et al. (2003) explore the challenges associated with protecting personal information and privacy in using location-based technologies, through the development of a system which provides individuals with control over how they disseminate location information. The authors claim that individuals must possess such control and be notified of requests to access information in order to maintain privacy. In the presented scenario, control would be compromised, with the emergent risks extending beyond privacy to lack of trust, suspicion, obsessive behaviours and fundamental consequences to the very nature of social relationships between individuals.

This encourages an enquiry into the nature of friendships where covert policing practices are employed in the community setting, posing the following central questions: To what extent is the boundary between the physical world, in which traditional friendships are forged, affected by the electronic world of GPS data logs and potentially incorrect location information? Given that friendships are built on trust, is this not an erosion of this fundamental core value?

3.5 Stranger-stranger

> *Scenario: Having recovered from his car accident, Benji had spent the last month afraid to leave his home. While his accident was minor and the damage to his car small, Benji was a little disconcerted about the small GPS tracker his mechanic found hidden under the body of his car. He lived in a friendly neighbourhood and knew almost everyone there, so who could have an interest in tracking his every move?*

The idea of being tracked by a third party in a public space is not new; however, with technologies capable of determining location with pin-point precision, the potential for third party tracking is increased, and to some degree facilitated. In a study which distinguishes between location tracking and position aware services, Barkhuus and Dey (2003) explain that location tracking services result in added privacy concerns, when compared to their position aware counterparts. That is, location tracking services require a third party to track the position of an individual, as opposed to position-aware services in which the device can determine its own location (Barkhuus & Dey, 2003). This finding was mentioned with reference to family and friends determining the physical position of an individual; inevitably the concerns increase when the idea of a stranger is introduced.

A recent study focusing on personal information in online social networks reported that individuals are generally unconcerned with friends accessing their profile, but expressed anxiety over other people viewing and retrieving personal information, the most concerning being those that the respondent is not acquainted with (Levin et al., 2008). When such a relationship is applied to the physical setting, and with the addition of mobile monitoring and tracking solutions, this interaction is represented by the stranger-stranger scenario.

The former scenarios have expressed the ease with which commercial solutions, such as GPS data logging devices, can be installed and utilised. These factors are highly attractive in the stranger-stranger situation, providing a vehicle for individuals to ascertain details about persons they do not know or are unfamiliar with, in a similar manner to what Benji experienced in the scenario. Such situations are typically characterised by malicious intent and involve improper conduct, usually of a deceptive nature. For instance, parents may seek location information to maintain the safety of their dependents. Similarly, friends may request geographic details for convenience purposes or to organise gatherings within their social network. However, in the stranger-stranger scenario, such motivations are invalid, as the concept of 'stranger'

itself suggests unfamiliarity, the unknown and the accessing of information without consent. This scenario demonstrates that the stranger-stranger interaction requires covert activity, deception and intrusion in its most basic form, due to the fact that individuals are unlikely to part with personal details, particularly location, to those they do not know. The 'intrusion' aspect or theme is further highlighted by the scenario, the outcome of such intrusion being fear and victimisation. Additionally, the installation of the device itself suggests that the 'victim' remains unaware of the activities occurring, another pivotal concern.

It is once again useful to look to social networking tools for insights into how emerging technologies are adopted by community members, as valid parallels can be drawn in the stranger-stranger scenario. This is applicable given the scenarios discussed throughout this paper are based on social interactions which are present and have become more clearly defined on social networking sites.

In a study which focuses on the features, history and literature regarding social networking sites, Boyd and Ellison (2008) identify the term networking to refer to the initiation of interactions between strangers; however, they go on to state that this is not the primary aim of such technologies. That is, social networking technologies are intended to support existing social networks, while encouraging and facilitating the ability for strangers to form connections based on some common interest. Importantly, the authors examine visibility and the public display of information as central themes within social networking technologies. In theory, these technologies provide users with the ability to grant and/or restrict access to their profile.

When such concerns are applied to GPS and location monitoring software, the nature of the terms are altered. That is, visibility and the display of information are now controlled by the individual who installs and possesses the device and related software, rather than the individual about whom the data is collected. Furthermore, the primary intention of monitoring and tracking solutions are to determine location, as opposed to forming networks and relationships (although solutions exist that provide both functions).

Consequently, the risks in the stranger-stranger situation are amplified, as they imply sinister notions such as stalking, sabotage, fraud, crime, and surveillance. These evident risks cannot readily be justified or masked in any way. Strangers are therefore empowered to perform covert policing techniques within the community setting, with the capability and tools to control or influence the behaviour of others. Such risks urge that safeguards be introduced to protect individuals from assuming the role of the victim is such a scenario. Further research is required to determine the intricacies of this stakeholder type, and to propose an enforceable strategy or legal framework that minimises the mentioned risks, and inhibits strangers from utilising mobile tracking and monitoring solutions for ill purposes. However, this remains a challenging area due to the difficulty in identifying offenders, and implementing pragmatic strategies that can be imposed on them.

4 Discussion and Conclusion

In drawing out the major themes from the scenarios and the related literature, it is valuable to consider the thought process underlying the concept of covert policing within a community setting. Figure 2 provides a summary of this process. The diagrammatic representation allows the following findings to be extracted: (i) the conceptualisation of the process, while applied to covert policing in this instance, is also applicable to other areas; (ii) in discussing the implications associated with emerging technologies, researchers and other individuals must consider the fundamental technical context, the social/environmental context in which the technologies are situated, in addition to the socio-ethical scenarios that will inevitably emerge; (iii) the implications recognised must take into account the positive applications, in conjunction to the less desirable effects, to ensure a balanced evaluation of the emerging technology; and finally (iv) further studies must consider the nature of the linkages between each of the identified elements and address the policy, regulatory and legal concerns.

Assessing the technical, social/environment and socio-ethical aspects allows us to draw a number of preliminary conclusions and themes from this present study. Firstly, GPS technologies contain vulnerabilities and are not error free. Thus in all scenarios, the 'victim' may be incriminated or judged based on incorrect information and evidence, in that inaccurate or false behavioural patterns may be revealed. That is, a digital chronicle of an individual may not necessarily match the physical reality, and thus assumptions cannot be made without accurate contextual information and discussions. Technological concerns aside, in applying solutions that were originally intended for law enforcement and covert policing purposes to the community setting, risks relating to relationships and interactions between stakeholders surface.

That is, the notion of covert activities implies deception and hidden agendas, which contribute negatively to social relationships. In cases where strangers are concerned, the issue is magnified and the psychological and legal ramifications are of primary importance. When individuals are acquainted, the issues are intricately linked to changing the nature of personal relationships, concurrent with previously discussed factors such as privacy, trust and control. All scenarios point strongly to the need for some form of protection, and the introduction of safeguards that would minimise the adverse consequences, which may come in the form of legal (regulation), ethical (safeguards and/or privacy policies), or technological (default features such as warning systems) mechanisms, in order to protect the interests of community members.

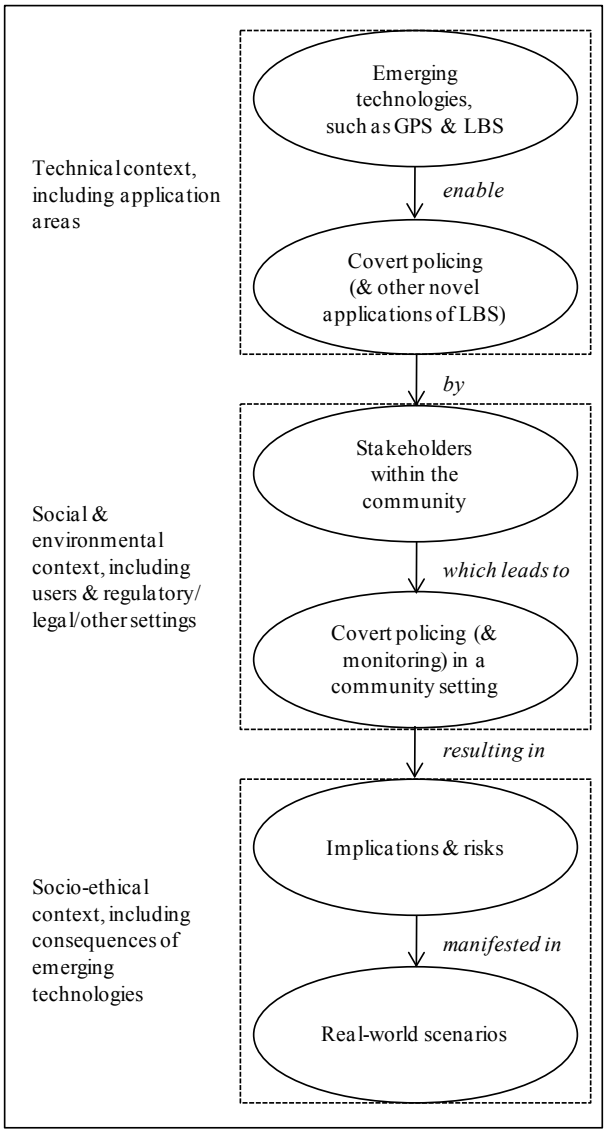


Figure 2: Conceptualising the notion of covert policing within a community setting

References

Barkhuus, L. & Dey, A. (2003), 'Location-based services for mobile telephony: a study of users' privacy concerns', *Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction,* pp. 1-5.

Barreras, A. & Mathur, A. (2007), 'Chapter 18. Wireless location tracking', in *Convenient or Invasive: The Information Age*, ed Larsen, K.R. and Voronovich, Z.A., Ethica Publishing, US, pp. 176-186.

Boyd, D.M. & Ellison, N.B. (2008), 'Social network sites: definition, history and scholarship', *Journal of Computer-Mediated Communication International Communication Association*, 13, pp. 210–230.
Chen, J.V. & Ross, W.H. (2007), 'Individual differences and electronic monitoring at work', *Information, Communication & Society*, 10(4), pp. 488-505.
Dobson, J.E. (2009), 'Big brother has evolved', *Nature*, 458(23 April 2009), p. 968.
Dobson, J.E. and Fisher, P.F. (2003), 'Geoslavery', *IEEE Technology and Society Magazine, Spring 2003*, pp. 47-52.
Ferenczi, P.M. (2009), 'You are here', *Laptop Magazine,* February 2009, pp. 98-102.
Herbert, W.A. (2006), 'No direction home: will the law keep pace with human tracking technology to protect individual privacy and stop geoslavery?', *I/S: A Journal of Law and Policy*, 2(2), pp. 409-473.
Iqbal, M.U. & Lim, S. (2003), 'Legal and Ethical Implications of GPS Vulnerabilities', *Journal of International Commercial Law and Technology*, 3(3), pp. 178-187.
Kaupins, G. & Minch, R. (2005), 'Legal and Ethical Implications of Employee Location Monitoring', in *Proceedings of the 38th Hawaii International Conference on System Sciences - 2005*, pp. 1-10.
Kerr, M., Stattin, H., & Trost, K. (1999), 'To know you is to trust you: parents' trust is rooted in child disclosure of information', *Journal of Adolescence*, 22, pp. 737-752.
Levin, A., Foster, M., West, B., Nicholson, M.J., Hernandez, T. & Cukier, W (2008), 'The Next Digital Divide: Online Social Network Privacy', *Ryerson University, Ted Rogers School of Management, Privacy and Cyber Crime Institute*, March 2008, www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf
Levin, A., Foster, M., Nicholson, M.J. & Hernandez, T. (2006), 'Under the radar? The employer perspective on workplace privacy', *Ryerson University*, www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf
Mayer, R.N. (2003), 'Technology, families, and privacy: can we know too much about our loved ones?, *Journal of Consumer Policy*, 26, pp. 419–439.
Michael, K., McNamee, A. & Michael, M.G. (2006), 'The emerging ethics of humancentric GPS tracking and monitoring', in *Proceedings of the International Conference on Mobile Business, Copenhagen, Denmark, 25-27 July 2006, IEEE Computer Society*.
Michael, M.G. & Michael, K. (2009), 'Uberveillance: microchipping people and the assault on privacy', *Quadrant*, LIII(3), 85-89.
Myles, G., Friday, A. & Davies, N. (2003), 'Preserving privacy in environments with location-based applications', Pervasive computing, Published by the IEEE CS and IEEE Communications Society, pp. 56-64.
Perusco, L. and Michael, K. (2006), 'The importance of scenarios in evaluating the socio-ethical implications of location-based services', *IEEE Technology and Society Magazine*, 2007, URL: http://works.bepress.com/kmichael/19/.
Schreiner, K. (2007), 'Where we at? Mobile phones bring GPS to the masses', *IEEE Computer Graphics and Applications*, ed Potel, M., May/June 2007, pp. 6-11.

Townsend, A.M. & Bennett, J.T. (2003), 'Privacy, technology, and conflict: emerging issues and action in workplace privacy', *Journal of Labor Research*, 24(2), pp. 295-205.

Weckert, J. (2000), 'Trust and monitoring in the workplace', in *Proceedings of the IEEE Symposium on Technology and Society, 2000, University as a Bridge from Technology to Society*, pp. 245-250.

11

E-policing and the social contract

Clive Harfield
Unversity of Wollongong

Abstract

The Age of Information has taken investigative and intelligence capabilities beyond the imaginations of Age of Enlightenment philosophers such as John Locke whose social contract theory of governance remains the moral justification for policing. Through philosophical analysis taking as its starting point John Locke, and philosophers of policing such as John Kleinig and Seamus Miller, this essay reflects on the basis of first principles whether the social contract theory remains valid in a governance environment characterized by digital identity and control of identity data. Specifically, it considers whether moral justification exists for criminal intelligence analyst access to data sharing, data matching and data mining techniques.

Keywords: social contract theory, e-policing information age

1 A rationale for policing

The policing of individual conduct in accordance with social conventions determined by democratic consensus derives its philosophical rationale from the work of John Locke (1690: chapters 2 and 9). If individuals are not to suffer the vulnerable and violent existence coincidental with a state of nature (being the consequence of the absence of government), if they are to enjoy the safety and society of communal living, then a degree of individual autonomy has to be surrendered in favour of executive authority invested in government. In democratic societies the justification for executive authority can be founded upon Locke's concept of the social contract theory of governmental authority: autonomous sovereignty is partially surrendered by individuals to representative government charged with protecting the interests of individuals accepting the authority of the government (see also Kleinig 2008:9-12).

Locke argued for a tripartite institutional framework to protect and promote mutual interests in an ordered society: "established standing laws" publicly debated and known, "indifferent and upright judges", and the "force of the community" to enforce the laws. [1] In practice representative assemblies denounce certain conduct as crime. Those who fall victim to crime are not left to their own devices: indeed the social contract demands that they do not take matters into their own hands. The force of the community made manifest in a police service or similar agency investigates the alleged crime on behalf of the victim (and society) and, having gathered evidence and identified a suspected perpetrator, presents both to an impartial fact-finding tribunal that determines on the basis of the evidence adduced: a) whether the alleged conduct took place; b) if so, whether the accused committed the conduct; and c) whether at the time of commission the accused had the necessary subjective criminal intent. Satisfaction on all three elements results in conviction. Conviction, in turn, results in social condemnation and, if deemed necessary by the indifferent and upright judge, punishment.

The state investigators are invested with certain coercive powers either fundamental to enforcement (detention, search and seizure, and arrest) or facilitating investigation (within the context of the considerations in this volume for instance, authority to conduct intrusive covert surveillance). Why are powers needed to fulfil the policing function? Not every member of society is persuaded by moral sentiment (Miller and Blackler 2005:27). Crimes are punished by imposing disadvantage or inflicting social and/or economic harm on the offender. Offenders disinclined to obey the law may reasonably be expected also to be motivated to evade punishment, particularly

1 "And so whoever has the legislative or supreme power of any common-wealth, is bound to govern by *established standing laws, promulgated and known to the people, and not by extemporary decrees; by indifferent and upright judges, who are to decide controversies by those laws; and to employ the force of the community at home, only in the execution of such laws, or abroad to prevent or redress foreign injuries, and secure the community from inroads and invasion. And all this to be directed to no other end, but the peace, safety, and public good of the people." John Locke, Second Treatise of Government, chapter 9, section 131, emphasis added.*

when it is likely to be severe. Thus for the law to be effective in maintaining social order as best possible it must be enforced upon individuals unwilling to accept its strictures. When non-compliance with the rule of law is encountered, authorities charged with enforcement must have recourse to coercion (such as arrest) and if necessary also the use of force (such as hand-cuffs applied to secure an arrested person).

The use of force and coercion to enforce the law is morally problematic (Miller and Blackler 2005:26). In the normal course of social interaction detaining a person, searching them and arresting them (each conduct against the will of the individual subject to it) are actions that are morally wrong; such conduct violates individual autonomy. Miller and Blackler provide the counter-argument to this objection: "These harmful and normally immoral methods are on occasion necessary in order to realise the fundamental end of policing, namely the protection of (justifiably enforceable) moral rights" (ibid.).[2]

Thus citizens have a legitimate expectation that, on their behalf, the authorities (to whom citizens cede some of their autonomy) will investigate and prosecute crime, having at their disposal means to do so denied to individuals pursuant to the social contract theory of government.

Further, the founding principles established with the statutory creation of the Metropolitan Police in 1829 illustrate a strong emphasis on *preventing harm, not just post facto remedy. "The basic mission for which the police exist is to prevent crime* and disorder", (principle 1); "Police use physical force to the extent necessary to secure observance of the law or to restore order *only when the exercise of persuasion, advice and warning is found to be insufficient", (principle 6, restricting the harm of police use of force); and "The test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with it", (principle 9, emphasising that the desired end is the outcome of prevention not the output of police action) (Grieve et al. 2007:36-7, emphasis added). To the citizen's legitimate expectation of investigation and prosecution thus may be added another: that government will seek to prevent harm, prevention being better than cure, the absence of crime and disorder being more conducive than the function of efficient investigation for the promotion of a mutually beneficial socio-economic environment.*

But this social contract was 'negotiated' at a time when the government's writ, if not actually still hand-written, was at best produced with ink and press. Does the reconfiguring of social and governance interaction through digital information warrant redefinition of the social contract of governance? This question arises from the fundamental difference between that which is now possible for government and citizen alike in the 'Age of Information', and that which was previously possible in the 'Age of Enlightenment' at a time when the emergence of the Westphalian state model first engaged philosophers such as Locke on the subject of the relationship between citizen and state (as opposed to the relationship between subject and sovereign). The parameters of potential state intrusion have been broadened. When

2 A search may be no less coercive simply because it is conducted covertly.

the Metropolitan Police was created 139 years after Locke published his second treatise on government, police potential for investigation was limited to documenting witness testimony and the seizure of physical items as evidence. The capacity for surveillance was limited at best to the natural capabilities of the human eye, perhaps reinforced through the power of a telescope, and those of the ear. What needs to be policed, and what can be investigated, have changed significantly since that time. Has so much changed that the justification for policing, and so the justification for methods that fulfil the purpose of policing, require revision?

2 Identity and autonomy

It has been argued that just as autonomy is a function of identity, so "anonymity is the basis of freedom in modern society" (Ogura 2006:274). The corollary to this is that (digital) identity has become the predominant mode of governance (Amoore 2008). Technological capacity for data collection coupled with the application of mathematical algorithms (Agrawal et al 1993), has extended the meaning of identity beyond simply the association of a biometric identifier with both a name and a physical address. Identity is no longer simply the information printed on a passport but the layers of databases accessed via computer screen linked to the name and biometric detail physically recorded (Amoore 2008:23). This makes possible the practice of überveillance (Clarke 2010; Michael and Michael 2010).

Commentators have reflected upon the implications of information communication technology [ICT] for identity and privacy with simultaneous awe and angst (Zureik and Salter 2005; Ogura 2006:277-80; Bennett and Lyon 2008; Mattelart 2010).[3] It is not the purpose of this paper to explore this aspect of the debate in detail suffice to note in passing one circumspect observation to which this argument will return: privacy is not the antidote to surveillance but is a framework against which authority can be held to account (Bennett 2005). Elsewhere there has been recognition that privacy in the Age of Information is as much in need of redefining as identity (Amoore 2008:32).

In the context of a social contract of government, control over personal data is both a means of governance for the authorities and an expression of autonomy for the individual. "On the internet, no one knows you're a dog" observed the *New Yorker cartoonist, Peter Steiner in 1993 (an era before Facebook offered a global public arena in which to design a specific self-presentation). An individual may legitimately have multiple identities.* [4] (Whether or not this is the basic right that some claim (Wigan 2010:35) or more an expression of autonomy is a debate for elsewhere.) Internet social-networking has given individuals significant control over the identity that they wish to present to others: the obverse is that such tools can be used by hostile others to

3 See also the various papers in Michael & Michael, (eds) 2006, 2007 and 2008.

4 A married woman, for instance, may use her maiden name for professional reasons and her married name in social contexts. Authors may use pseudonyms under which to write books from different genres.

manipulate identities so posted. Identities can be manufactured, stolen or maliciously manipulated in ways and on a scale unprecedented before the availability of ICT. Customer purchase data collated (and traded) by commercial organizations creates another 'identity' for an individual: their commercial footprint. Behaviour patterns are discerned and sophisticated analysis used to inform strategies of influence and subliminal persuasion with respect to future purchasing behaviour; ethnographic marketing so-called, based on spending data and devices such as hidden cameras to monitor customer reactions to shop displays (Mattelart 2010:193). The customer is complicit in the creation of such an identity (store loyalty cards are voluntary, so is use of credit cards)[5], and in exchange for data which enables the creation of this identity the customer is 'rewarded' (some would argue bribed or intimidated (Martin 2010) with greater shopping convenience, such as targeted advertising when their mobile phone enters an area in which are located shops that might be of particular interest.

Threats to modern (territorially-based and therefore geographically static) governments are mobile in character. Terrorism is of no fixed abode and frequently targets, or else exploits, transport systems to maximise hostile impact with physical and psychological harm. Irregular population movements and illicit migration challenge government control of the population. Organized crime exploits the global economic market -flows both to generate profit through the provision of illegal goods and services and then to infiltrate that profit into the legitimate economy through money laundering (UN 2010:18; 21; and 29 for instance). Inability to police persons, goods and financial transactions inhibits government ability to raise fiscal revenue and promote socio-economic wellbeing through good order (accepting the premise that such continues to be the role of government). Monitoring movements of persons, goods and money is an inevitable and fundamental tool in preventing and prosecuting criminality that seeks to exploit such movements. The deal by which individuals trade certainty of identification (thus facilitating official monitoring of their movements) for relatively uninhibited mobility (Amoore 2008:28) may be seen as a modern expression of the social contract. In this updated 'contract', in which governments provide a secure mobility environment though mechanism such as vehicle safety regulations for cars, trains and planes for instance, individuals complying with the monitoring of behaviour (either by commercial or government interests) continue to concede some of their autonomy.

In breaking the law criminals rely on anonymity, the non-discovery of informational linkages and the non-discovery of information about the crime and/

5 There comes a point, of course, when devices such as credit cards are promoted to the point of such ubiquity that not having one inconveniences an individual by excluding them from optimal socio-economic interaction.

or their role in the crime in order to evade prosecution and frustrate good order.[6] The right to control information about oneself is an inherent characteristic of individual autonomy – although the related right to privacy is not the same thing as the moral right to be autonomous (Miller and Blackler 2005:84). These two rights are at odds with the competing right of victims to live autonomously, free from the harm of crime and the right to be protected by the state from crime. A right of total autonomy is constrained by the obligation not to cause (or condone) harm to others. It exists within a moral context in which protection from harm is a legitimate community and individual expectation. The rights of victims to be protected from crime through the prevention or prosecution of crime are held to out-weigh the right of suspected criminals to privacy, to the extent that intrusion against privacy is necessary to understand criminal and social harm and so inform a preventative intervention or to secure evidence to put before a trial for due consideration. In investigating suspected criminality, either to prevent or prosecute its occurrence, police may legitimately be expected to explore all lawful avenues of enquiry and are justified in doing so in order to fulfil the policing purpose. [7]

3 Policing risk and harm through strategic data analysis

At issue is not the tool (data collection) but the use to which the tool is put (data analysis). Analysis could be undertaken in a way that violates autonomy beyond reasonable use and expectation so harming an individual. Equally, in the context of governments managing risk to achieve a safe society, such data arguably is being used to preserve autonomy by securing the safe environment within which autonomy is optimally exercised. The security alternative to freedom of movement subject to identity checks is reduced or no freedom of movement. The alternative to security is insecurity. Between these polar opposites operates a scaled continuum of confidence. It is the perennial paradox of policing: police can serve or suppress, protect or prejudice. The fact that harm might arise from misuse is not an argument for prohibition of use. It is an argument for use management; and argument for restraining the authoritative autonomy of officials through principles enshrined in rules (Galligan 2007:234-6).

The conceptualization of national security is changing. No longer is it seen as exclusively the protection of state institutions from an enemy's hostile attention. The concept has been extended to protecting the citizen from risks that defy individual

6 Hakan Ayik, at time of writing a fugitive from Australian law enforcement, keeps police updated about his non-extraditable whereabouts and criminal lifestyle via Facebook: 'Crime Incorporated', ABC Four Corners, broadcast 30th August 2010 on ABC1, http://www.abc.net.au/4corners/content/2010/s2994584.htm (accessed 3rd December 2010).

7 That which is lawful or unlawful is a construction of the relevant legislature. If an issue is not specifically prohibited or positively enacted it is often held to be lawful until specifically prohibited.

response and so demand government resources to mitigate (Omand 2010). [8] In this configuration organized crime can be viewed as a threat to national security (so redefined) (Cabinet Office 2008). Often studied in the transnational context (for example Irrera 2010), organized crime nevertheless has adverse impact on local communities (Hobbs 1998). It has consequence from the international to the individual, from state and society to the citizen.

Omand identifies a three-phase strategy for securing a nation and protecting its citizens from risks and vulnerabilities against which as individuals, they can do little about: a) adopt an all-risks approach; b) anticipate the risks; and c) establish and maintain a resilient society. The first is a matter of political will. The second two require strategic intelligence. Reviewing prevailing police contribution to strategic intelligence about crime, Ratcliffe and Sheptycki observe that "the entrenched law enforcement sub-culture of the police sector shapes the [criminal] intelligence process in ways that undermine the strategic view" (Ratcliffe and Sheptycki 2009:261). This is because the dominant detective culture is built around investigation, arrest and prosecution and in this context intelligence is seen merely as a facilitator of detection. Such a narrow focus severely constrains police contribution to the prevention of crime because, as recidivism figures demonstrate, crime control through prosecution all too often has little deterrent effect as a means of preventing individuals from committing crime. [9] The narrowness of this focus is reinforced in a view of data control which denies police access to data held by other government agencies that is capable of informing a wider understanding of criminal harm. The value of truly strategic intelligence, in the view of Ratcliffe and Sheptycki, is that it provides the basis for meaningful impact analysis (2009:253) and so serves the needs of harm-based modelling which is increasingly coming to be recognised as a more promising approach to addressing the range of social problems to which crime (and some exclusively law enforcement solutions) gives rise (Hillyard and Tombs 2007; Ratcliffe and Sheptycki 2009:262-3).

Because strategic impact assessments are not offence-specific (Ratcliffe and Sheptycki 2009:252), and because there is, at the level of serious enterprise crime, a blurring of the distinction between licit and illicit conduct, there is a need to set intelligence about crime (as distinguished from intelligence about criminals) alongside the data gathered by other government agencies. In this regard, the potential exists for government agencies and law enforcement to utilise data sharing, matching and mining techniques across multiple databases for harm identification and minimisation in the same way in which commercial organizations use (and

8 The identification and categorization of risk is potentially controversial, and a debate beyond the scope of this essay. For the purpose here let benign and proper motivation be presumed.

9 In an unrestricted, but unpublished, submission to the 2001 review by Lord Auld of the English criminal justice system, the Association of Chief Police Officers of England and Wales asserted "… the rate of attrition to organized crime *[from prosecution] is so small that it represents little threat' [to the criminals]*, para. 6.2.

indeed developed) such techniques for the purpose of profit maximisation (House of Lords 2009:paragraph 93). [10]

Harmful impact, beyond individual victimisation, has proved elusive to quantify (Home Office 2004) although instinctively and intuitively governments and citizens recognise that individual victimisation represents just the tip of the ice-berg. The true nature of harm to the economy and economic infrastructures from organized crime, for instance, is unlikely to be evident from police criminal intelligence databases: it will emerge from those databases that hold information about the economy, about financial transactions (hence widespread requirements to report suspicious transactions), and about the health of the community (in relation to issues arising from drug, alcohol and tobacco addiction, notwithstanding that the latter two are also legally available as well illicitly available).

If, through meta–analysis government could anticipate current and emerging risks more accurately, if as a consequence prevention intervention could be initiated that minimised potential harmful impact, why would (or should) government agencies not undertake such analysis given that citizens have yielded a degree of individual autonomy in exchange for government protection from what might be termed mega-risks? [11] A philosophical proposition may be asserted that law enforcement intelligence agencies should be empowered to conduct data sharing, matching and mining and meta-analysis because it is necessary to identify and so protect against strategic crime harms.

4 Objection and rebuttal

A number of objections can be raised to this proposition – but to each there may also be made argument in rebuttal.

The first objection is that the gathering of personal data by governments is an affront to individual autonomy. In rebuttal it may be argued that individuals wishing to enjoy the protection of an orderly society necessarily concede a degree of autonomy but volunteering – and expecting others to volunteer – to be restrained by social values ands conventions, many of which find expression in laws enforced by government: government enforcement of law being preferred to individuals taking the law into their own hands.

The second objection follows on from the first. Dataveillance – to use Clarke's pre-requisite concept underpinning Michael's emergent notion of überveillance (Clarke 2010; Michael and Michael 2010) – represents a degree of intrusion against the individual that is unreasonable. In rebuttal it may be argued that degrees of criminal harm have also intensified. ICT and emergent technologies such as cloud computing (Choo 2010) expand the capacity and capabilities of criminal enterprises as much as those of legitimate small and medium-sized enterprises or multi-national

10 Harm identification and minimisation is understood to extend in potential beyond the investigation and prosecution of prolific criminals.

11 A mega-risk is taken to be a risk beyond the scope of an individual to mitigate.

corporations. Individual criminals or criminal networks are now capable of causing more harm to more victims than before. Within the social contract, the right to be protected from crime has hitherto outweighed rights of privacy, witness the qualified right to respect for private life protected under Article 8 of the European Convention on Human Rights and Fundamental Freedoms 1950. In this construction enhanced data analytical ability does not, in and of itself, negate or provide reason to reverse, the balance between the relative rights of privacy and non-victimization that prevail. *The fact that meta-analysis may be used to conduct previously unachievable mass surveillance, and so generate suspicions where none previously would have arisen, is a third objection. It can be argued, for instance, that mass surveillance through data sharing, matching and mining violates Article 17 of the International Covenant on Civil and Political Rights 1976, which asserts as an international norm that there should be no arbitrary government interference with an individual's privacy, family or correspondence (the closest equivalent in the ICCPR to Art. 8 ECHR). Rebuttal may be made in two parts. One function of strategic intelligence analysis is to identify the need for tactical intervention. Thus identified on the basis of verifiable need or reasonable suspicion such interventions by definition are not arbitrary but based on evidenced decision-making which may be held to account.*[12] Secondly, much of the criminal profit derived from organized crime, including computer-enabled crime, is often characterized as being victimless. This does not, of course, mean that there are no victims merely that these are crimes in which the historical model of victim allegation as trigger for official investigation may not or does not apply. That is no reason not to investigate and prevent criminal harm. It is generally accepted that crime harms society as much as individual citizens within a society. A citizen's right and legitimate expectation to be protected from crime by government imposes on government a duty to take measures reasonable within the social contract to prevent crime as well as investigate and prosecute such conduct when it has not been prevented.

The system can be abused of course and herein is to be found a fourth objection. Data sharing, matching and/or mining can be used inappropriately. Any authoritative power or capability can be. The harms to individuals arising from unjustifiable meta-analysis could include the creation of adverse digital identities which are then used as the basis for unfair discrimination and denial of access, advantage or benefits that would otherwise be legitimate. But that is insufficient to deny the use of such analysis as a means of identifying and preventing harm. It is sufficient to warrant restraints being placed upon agencies with access to such capabilities. Restraint on officials is achieved through principle-based rules, the definition of acceptable use, the delegation and diffusion of authority and lines of accountability (Galligan 2007:235-6). Which brings the discussion back to the notion introduced briefly

12 Parameters of reasonable suspicion have been drawn in statutory codes of practice and case law: *Police & Criminal Evidence Act 1984 (England & Wales), Code of Practice A - Stop and Search (as amended in 2009), paragraphs 2.2 to 2.11; in Australia see R v Rondo* (2001) 126 A Crim R 562 at [53].

above that privacy is not the antidote to surveillance but is a framework against which authority can be held to account (Bennett 2005).

The fifth objection relates directly to the fourth because meta-analysis through data sharing, matching or mining of multiple databases overcomes the very mechanism of restraint provided by the diffusion and delegation of authority through which, for example, data relevant to fiscal management is restricted to revenue agencies, and data relevant to criminal investigation is restricted to law enforcement agencies. Data collected for one purpose should not, the argument holds, be used for another. This cannot be rebutted merely by recourse to the platitudinous and anodyne rhetoric of 'joined-up government' or a 'whole of government' approach. The problem that does confront such objection, however, is the increasingly blurred and imprecise distinction between illicit and legitimate conduct. Money laundering is a case in point. The purpose of money laundering is to facilitate and disguise the transition of criminal profit into the legitimate economy. Such transition undermines the value and integrity of the legitimate economy and thus is a source of significant social harm. No responsible government can ignore the problem. It is a problem the nature of which must be capable of recognition and comprehension through data analysis. Inevitably the investigation of money laundering and similar 'grey' conduct straddling the divide between criminal and lawful conduct necessitates analysis of data relating to lawful activity that has been gathered for regulatory purposes rather than for law enforcement purposes. Such is the harm that must be countered, it is necessary to adapt the diffusion and delegation of authority comprising one of Galligan's restraints on officialdom from an agency focus to a functional focus. The merging of the licit with the illicit, the fact that legitimate conduct is used to facilitate and/or disguise criminal conduct – hiding criminality in plain sight – is itself a significant harm. It warrants regulated analysis of the legitimate alongside criminal intelligence analysis in order to recognise the vulnerabilities and harms. To reinforce restraint through accountability it may be necessary to create analytical or intelligence agencies specifically for this purpose rather than empower existing law enforcement agencies, thus re-converting the functional focus back into an agency focus but at the risk (which must be countered through strong governance and accountability) of creating a powerful agency that uses data protection and security arguments as a justification for secrecy and resistance to governance. [13]

A final objection can be posited that meta-analysis facilitates the evolution of governance by überveillance into a surveillance society which will eventually

13 "The formulation of law is hard enough, designing suitable organizations and their institutional base, even harder …" (Galligan 2007:235). In the UK the National Criminal Intelligence Service was an agency avowedly and by design independent of the investigation and prosecution function until its 2006 incorporation into the Serious Organized Crime Agency which also had law enforcement and investigative functions. The Australian Crime Commission is a variant on the model although the fact that its governing board comprises law enforcement commissioners undermines any argument that the ACC is truly independent from police agencies.

reduce individual human identity into a single, unique digital identifier through which autonomy is all but eradicated; the notion of society as an interaction of individual citizens all but destroyed (to recognise and echo the sometimes shrill rhetoric of opponents of surveillance: for example Martin 2010). Such an apocalyptic outcome may be resisted by not creating unique individual digital identifiers, and not embarking on systems of government that only function on the basis of such unique identifiers. But if such an outcome is resisted than, by definition, in a world in which ICT is used to commit significant crime and cause significant harm, there must be a mechanism for those charged with preventing such harm or prosecuting its occurrence to identify the same through strategic analysis. In such a construction the capacity to undertake meta-analysis through data sharing, matching and mining becomes the reason that a unique digital identity is not necessary.

5 A new social contract?

Such moral analysis provides no compelling argument to negate or invalidate the presumptions underpinning the social contract theory of government as currently practised.

The fact that objections to the proposition can be rebutted however, does not deny the legitimacy of concerns surrounding the potential use to which digital data could be put by government agencies, commercial enterprises and criminal networks. Addressing such concerns has not been the principal purpose of this essay but that is not to say that such concerns are not important. The focus here has been to review whether changes in the technology of information have changed the social context to an extent that justifies a 'renegotiation' of the social contract of governmental theory upon which the rationale for policing is based.

The investigation of alleged crime and the prosecution of suspects is one activity through which the police seek to achieve the overarching purpose of policing (Miller, Blackler et al. 2006:45). A (potential) victim of crime has a moral right not to have their peaceful and secure autonomy violated by a criminal act. In the first instance there is a legitimate expectation that authorities which purport their role to be one of securing public safety should act to prevent crime where possible. When such violation occurs, victims have a right in the form of a legitimate expectation that police will do everything in their lawful power to detect the crime, identify the offender and prosecute.

The fact that ICT in the Age of Information necessitates reconsideration of the meanings of identity, privacy and autonomy does not, in and of itself, dictate a change in the moral justification for policing (or functions that fulfil its purpose) as a means of protecting a citizen's justifiably enforceable moral rights. Alongside the changes in technology and enhanced realisation of the power of data analysis has come recognition that sustainable impact on crime as a social problem (in all of the international, transnational and domestic arena) is more important than prosecution of individual criminals (the value of which even police practitioners

are openly questioning in relation to serious organized crime: ACPO 2001). To achieve sustainable impact, harm-based modelling is necessary. To achieve harm-based modelling, data sharing, matching and mining are necessary.

Let it be clear what is NOT being argued here. No attempt is being made here to deny the need for regulated use of such methods by the authorities. Appropriate restraint on officialdom reinforces of the legitimacy of officialdom and its functionaries (Galligan 2007:234-6). Just as due process protections act to redress the asymmetrical power relationship operating when an individual is put on trial by the state, so information management regimes (data protection, freedom of information, regulated access to information gathering methodologies) can serve to prevent unwarranted use of data. Critics such as Martin would, apparently, object on the basis that such an argument is merely re-interpretative 'spin' (2010:27). But within the social contract theory of government that is the deal: responsible and regulated use of the authority ceded by the individual choosing to live within a governed society to the government. In return for which the individual legitimately expects government to do what it reasonably can to protect the individual from harm such as crime, particularly when the threat and risk of harm is beyond the capacity of the individual to mitigate (as, for example, with transnational organized crime). Remedy is properly instituted in the event that government or its agencies abuse the power invested in them. If it is to be argued that governments and agencies such as the police should not use data sharing, data matching and data mining in the ways in which such methods can be used for social good, then the onus is placed on those making such arguments to justify why government should not protect the individual and wider society from harm: which would indeed require rewriting the social contract.

Chesterman argues that a new formulation of the social contract is emerging in which granting of access to information earns increased security and convenience in daily life (2011:250). The key difference is the new rage of actors to whom concession is made and from whom benefit is received (ibid:252). This is a function of economic globalization beyond the direct control of governments and of increased outsourcing by governments of sub-contracted government functions. The ambiguity between public and private in these circumstances is one that obscures the clarity of Locke's vision but does not divert it. The obscurity may be overcome with transparency of the powers being used. This is one of three principles postulated by Chesterman for modernising the historical contract. The second principle is legality and the third accountability for use made of analysed data (rather than accountability of who accesses the data) (ibid. 254-6). Reconfiguring regulation in this way does not alter the basic premise of the contract and does not alter the arguments privileging protection from crime victimisation over private interest.

6 Conclusion

The emergence of ICT per se does not alter the moral rationale inherent in

Locke's social contract. The context is based on an individual's relationship with government which is expressed through the mechanism of identity. The notion of identity is increasingly complex in the Age of Information. It can be viewed from the perspective of privacy and autonomy. However, in terms of moral justification for police agency data sharing, matching and mining in collaboration with other agencies, the primary moral issue is not one of privacy or autonomy but whether protection of a third party's privacy outweighs the moral right of a potential victim of crime not to have their peaceful and secure autonomy violated by a criminal act. The first principles approach applies to the relationship between a citizen and the political state of which they are a citizen, which has been the focus of this paper. No attempt has been made here to explore the complications which arise when a citizen's government shares identity data with foreign governments with whom, by definition, the citizen has no social contract relationship. Suffice it for the time being to observe here that a citizen may legitimately expect the government to do what it can to protect citizens from transnational crime as well as from purely domestic crime. Considerations about the philosophical rationale for policing within the context of transnational interaction and international relations require a paper in their own right.

At a time when so many observers are trumpeting the potential harm arising from the State's access to data, it is worth recalling that there is a social good as well as individual harms that can come out of such access.[14] Increased use of data analysis may inherently harm the concept of individual privacy but as Miller and Blacker noted a lesser moral harm is sometimes necessary to achieve a greater social good (2005:26). ICT has, arguably, given government more power in monitoring and influencing individual autonomy. Equally, ICT has given individuals more ways of expressing and exploiting autonomy. Exponential increase in capacity on both sides of the debate does not appear, on this analysis, to justify reframing the debate outside Locke's social contract.

References

ACPO (2001). Written submission to the review of the criminal justice system in England and Wales undertaken by Lord Auld. (Unpublished).

Agrawal, R, Imielinski, T & Swami, A. (1993). 'Mining association rules between sets of items in large databases' *SIGMOD Proceedings, pp.914-25*

Amoore, L. (2008). Governing by identity. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, in C. Bennett and D. Lyon (eds), Abingdon, Routledge**:** 21-36.

Bennett, C. (2005). What happens when you book an airline ticket? The collection and processing of passenger data post 9/11. *Global Surveillance and Policing: Borders, Security, Identity*. E. Zureik and M. Salter. Cullompton, Willan**:** 113-138.

14 A useful summary, with documented evidence from both sides of the argument, is presented in House of Lords 2009.

Bennett, C. and D. Lyon, Eds. (2008). *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. London, Routledge.
Cabinet Office (2008). *The National Security Strategy of the United Kingdom: security in an interdependent world*. Cabinet Office. London, TSO.
Chesterman, S. (2001). *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty*. Oxford, Oxford University Press.
Choo, K.-K. (2010). "Cloud computing: challenges and future directions." *Trends and Issues in Crime and Criminal Justice*(400): 1-6.
Clarke, R. (2010). "What is überveillance? (And what should be done about it?).» *IEEE Technology and Society Magazine* 29(2): 17-25.
Galligan, D. (2007). *Law in Modern Society*. Oxford, Oxford University Press.
Grieve, J., C. Harfield, & A. MacVean. (2007). *Policing*. London, Sage Publications.
Hillyard, P. and S. Tombs (2007). "From 'crime' to 'harm'." *Crime, Law and Social Change* 48: 9-25.
Hobbs, D. (1998). "Going down the glocal: the local context of organized crime." *The Howard Journal of Criminal Justice* 37(4): 407-422.
Home Office (2004). *One Step Ahead: A 21st Strategy to Defeat Organised Crime*. Home Office. London, TSO.
House of Lords (2009). *Surveillance: Citizens and the State*. Select Committee on the Constitution. HL Paper 18-I, Second report of the session 2008-09, London, TSO.
Irrera, D. (2010). Transnational organized crime and the global security agenda: different perceptions and conflicting strategies in *Defining and Defying Organized Crime: Discourse, Perceptions and Reality*. F. Allum, F. Longo, D. Irrera and P. Kostakos (eds). Abingdon, Routledge**:** 71-84.
Kleinig, J. (2008). *Ethics and Criminal Justice: An Introduction*. Cambridge, Cambridge University Press.
Locke, J. (1690). *Second Treatise of Civil Government*. London.
Martin, B. (2010). "Opposing surveillance." *IEEE Technology and Society Magazine* 29(2): 26-32.
Mattelart, A. (2010). *The Globalization of Surveillance*. Cambridge, Polity.
Michael, K. & Michael, M. (2006). *The Social Implications of Information Security Measures on Citizens and Business*. Wollongong, University of Wollongong.
Michael, K. & Michael, M. (2007). *From Dataveillance to Überveillance and the Realpolitik of the Transparent Society*. Wollongong, University of Wollongong.
Michael, K. & Michael, M. (2008). *Australia and the New Technologies: Evidence Based Policy in Public Administration*. Wollongong, University of Wollongong.
Michael, M. and K. Michael (2010). "Toward a state of uberveillance." *IEEE Technology and Society Magazine* 29(2): 9-16.
Miller, S. and J. Blackler (2005). *Ethical Issues in Policing*. Aldershot, Ashgate.
Miller, S., J. Blackler, & Alexandra, A. (2006). *Police Ethics*. Winchester, Waterside Press.
Ogura, T. (2006). Electronic government and surveillance-oriented society, in *Theorizing Surveillance: The Panopticon and Beyond*. D. Lyon (ed). Cullompton, Willan**:** 270-295.
Omand, D. (2010). *Securing the State*. London, Hurst and Company.

Ratcliffe, J. and J. Sheptycki (2009). Setting the strategic agenda, in *Strategic Thinking in Criminal Intelligence*. J. Ratcliffe (ed). Sydney, The Federation Press: 248-268.

United Nations (2010). *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. Vienna, UNODC.

Wigan, M. (2010). "Owning identity - one or many - do we have a choice?" *IEEE Technology and Society Magazine* 29(2): 33-38.

Zureik, E. and M. Salter, Eds. (2005). *Global Surveillance and Policing: Borders, Security, Identity*. Cullompton, Willan.

12

The Practical Effects of the Human Rights Act 1998 on Policing in England and Wales

Nick O'Brien
Charles Sturt University

Abstract

The Human Rights Act (HRA) 1998, based on the European Convention on Human Rights, had a dramatic impact on policing in England and Wales. In terms of privacy, the Act imposed a requirement for police and other investigatory bodies to formally consider such aspects as proportionality prior to taking actions which could be considered intrusive. Prior to this legislation, in simple terms, police could take any actions they considered necessary as long as there was not legislation forbidding those actions. Cost rather than proportionality was a major consideration when decisions were made to undertake intrusive investigations. The Regulation of Investigatory Powers Act (RIPA) 2000 was introduced as the legislation which enabled investigatory bodies to conduct intrusive investigations. RIPA and the HRA imposed a significant bureaucratic and therefore cost burden on police. Despite this, the author who was a serving police officer at the time, supports the introduction of the legislation and recommends that jurisdictions considering introducing similar legislation should examine the UK experience.

Keywords: human rights act, England and Wales policing

In this chapter I will discuss the practical effects of the Human Rights Act 1998 on policing in England and Wales and also make some comments about the European Court of Human Rights in Strasbourg. These issues are both discussion points rather than in-depth analyses and I hope that it will provoke some interesting discussions about the issues raised.

The issue of human rights legislation in Australia is currently exercising the mind of academics, legislators, bureaucrats, lawyers and other interested parties. A Committee has been appointed by the Australian Government to, "undertake an Australia-wide community consultation for protecting and promoting human rights and corresponding responsibilities in Australia" ("Human Rights Committee Terms of Reference," 2009). The Committee will report to the Australian government by 31st August 2009.

The UK introduced human rights legislation in the late 90s. In the case of the UK the issue of what needed to be in the legislation was relatively simple. The Human Rights Act 1998 was based on the European Convention on Human Rights which the UK ratified in 1951 (Wadham & Mountfield, 1999, p. 10) but did not incorporate into law. There effect of the non-incorporation was that the use of the Convention was 'limited to cases when the law was ambiguous' (Wadham & Mountfield, 1999, p. 2).

The introduction of the Human Rights Act (HRA) had an enormous affect on British policing. Indeed, the preface to Blackstone's Guide to the Human Rights Act 1998 stated that, "The Human Rights Act 1998 will have a momentous impact on our legal system. It is the most important piece of constitution legislation in Britain for many years. It will affect every area of law in England and Wales and also on Northern Ireland and Scotland. No law student or legal practitioner will be able to ignore its effect" (Wadham & Mountfield, 1999, p. xi). As a police officer at the time of the introduction of the Act I can attest to the accuracy of that comment.

So what did it change? In simple terms prior to the HRA the British police could do what they wanted as long as there was not a law forbidding it or regulating it in some other way. So for example if an investigating officer wanted someone followed or photographed a request was made to the surveillance squads who carried out that request. There was management oversight but that oversight was mainly confined to cost issues and to what work should be given priority. Common sense did prevail and sixteen person surveillance teams were not used to follow people suspected of shoplifting. A person's right to privacy however was not one of the issues that managers considered prior to authorising intrusive actions like surveillance or the use of what became know as Covert Human Intelligence Sources or CHISs. In popular parlance a CHIS is an agent or informer.

The provisions of the HRA meant that instead of police being able to do anything intrusive unless there was a law prohibiting it, police could now only take action if there was legislation that permitted that action. This meant that new laws were needed to enable police to investigate offences. So the Regulation of Investigatory

Powers Act 2000 was introduced which governed investigations by the Security Service and other government departments as well as the police. The Regulation of Investigatory Powers Act was known as RIPA and inevitably came to be called the 'Grim RIPA' by many police officers.

The UK's Home Office which is the approximate equivalent of the Attorney General's Department in Australia makes the following comments about RIPA.

About the Regulation of Investigatory Powers Act

The Regulation of Investigatory Powers Act 2000 (RIPA) puts a regulatory framework around a range of investigatory powers.This is done to ensure the powers are used lawfully and in a way that is compatible with the European Convention on Human Rights. It also requires, in particular, those authorising the use of covert techniques to give proper consideration to whether their use is necessary and proportionate.

RIPA regulates the following areas:

- The interception of communications (for instance, the content of telephone calls, e-mails or postal letters)
- The acquisition and disclosure of communications data (information from communications service providers relating to communications)
- The carrying out of covert surveillance
  - in private premises or vehicles ('intrusive surveillance') or
  - in public places but likely to obtain private information about a particular person ('directed surveillance')
- The use of covert human intelligence sources (such as informants or undercover officers)
- Access to electronic data protected by encryption or passwords.

RIPA provides a number of important safeguards:

- It strictly limits the people who can lawfully use covert techniques, the purposes for and conditions in which they can be used and how the material obtained must be handled
- It reserves the more intrusive techniques for intelligence and law enforcement agencies acting against only the most serious crimes, including in the interests of national security
- It provides for the appointment of independent oversight Commissioners and the establishment of an independent tribunal to hear complaints from individuals who believe the techniques have been used inappropriately (*About RIPA*, 2009).

Two of the most important words in the Home Office's comments are 'necessary' and 'proportionate'. Are investigative methods which invade the privacy of the

suspect necessary? The right to privacy is enshrined in Article 8 of ECHR which states, 'Everyone has the right to respect for his private and family life, his home and his correspondence' ("Convention for the Protection of Human Rights and Fundamental Freedoms," 1950). In other words will the investigations tend to prove or disprove the case and are there other methods of finding out the information. It is important to emphasise that the rights enshrined in ECHR are not absolute rights. For example I have mentioned Article 8, the right to a private life. Article 8 also goes on to state,

> 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others' ("Convention for the Protection of Human Rights and Fundamental Freedoms," 1950).

This is not a 'get out' clause for governments, instead it requires investigating agencies to exercise a degree of judgement and under RIPA to record that judgement and to have it scrutinised by Surveillance Commissioners.

The issue of 'proportionality' is key to operating under a Human Rights framework. Working in the area of counter-terrorism, proportionality isn't too much of an issue because terrorists want to kill, therefore a wide variety of intrusive investigative methods would be proportional in the eyes of the Surveillance Commissioners. However in some other areas the issue is not so clear. I would guess that most people here would consider that it would not be proportional to put listening devices in the home of a person who is stealing food from shops. Most people might also think that it would be proportional to put listening devices in the home of someone planning a multi-million dollar armed bank robbery. The issue then becomes, 'when do you cross the line?' Is it when the robbery is over a million or is it the use of weapons in a robbery? Deciding when something is proportional is not an exact science. Rather it is a matter of judgement but that judgement will be informed by the past comments of the Surveillance Commissioners.

European Court of Human Rights

> When individuals believe that their Human Rights have been breached they may take their cases to the European Court of Human Rights in Strasbourg. On 19th March 2009, the second most senior Law Lord in the UK, Lord Leonard Hoffmann delivered a lecture to the Judicial Studies Board and some of his comments about the court are scathing. Its worth paying heed to what Hoffmann says so that we can avoid making the same mistakes. Hoffmann comments that as of November 2008, the court had a backlog of some 100,000 cases which represents 4 years work. He identifies the problem stating that, 'the court has no

> summary mechanism for dealing with hopeless cases. Every petition properly filled in must go before a committee of 3 judges and then, if admissible, before a committee of 5' (Hoffmann, 2009). Examination of the court's own websites reveals that Hoffmann has a point. In 1999 8,408 cases were allocated to a decision body. In 2008, up to 1st November, 42,376 had been allocated to a decision body. With the exception of 2003, the number of cases allocated had risen in every year since 2008 (*European Court of Human Rights Facts and Figures 2008*, 2008). Hoffmann comments that, unless something is done, 'the court will drown in its own workload' (Hoffmann, 2009). We have all heard the saying that 'justice delayed is justice denied'. That certainly seems to be the case with the Strasbourg court and we must make sure that we do not make the same mistakes in Australia if we go down the route of a Human Rights court.

To conclude I want to make some remarks about the HRA and its introduction in the UK. It was a pain. It tripled paperwork, costs millions in extra staff hours, IT systems and took a number of years before it was properly understood. As an authorising officer for both Surveillance and Covert Human Intelligence Sources I witnessed the frustrations of trying to deal practically with the HRA and RIPA. Despite all that I believe that it was the right thing to do. Human Rights are important in a democracy and investigating agencies should consider proportionality in their investigations. It also focussed our thinking and I am sure that we saved money by not using expensive surveillance when we would have done in the past. If similar legislation is introduced in Australia we will need a good lead in time to ensure that the legislation is understood. Above all we must look to other countries that have introduced human rights legislation to examine what went wrong so that we minimise the chance of making the same mistakes.

References

About RIPA. (2009). Retrieved 6th April 2009. from http://security.homeoffice.gov.uk/ripa/about-ripa/.

Convention for the Protection of Human Rights and Fundamental Freedoms, (1950).

European Court of Human Rights Facts and Figures 2008. (2008). Strasbourg: European Court of Human Rights.

Hoffmann, L. (2009). The Universality of Human Rights: Judicial Studies Board.

Human Rights Committee Terms of Reference. (2009). Retrieved 6th April 2009, 2009, from http://www.humanrightsconsultation.gov.au./www/nhrcc/nhrcc.nsf/Page/Terms_of_Reference

Wadham, J., & Mountfield, H. (1999). *Blackstone's Guide to the Human Rights Act 1998*. London: Blackstone Press Limited.

13

The European Court of Human Rights Ruling against the Policy of Keeping Fingerprints and DNA Samples of Criminal Suspects in Britain, Wales and Northern Ireland: The Case of S. and Marper v United Kingdom

Katina Michael

University of Wollongong

Abstract

In England, Wales and Northern Ireland, the Police and Criminal Evidence Act 1984 (the PACE) contained powers for the taking of fingerprints, and samples in the form of deoxyribonucleic acid (DNA). In 2001, Section 64(1A) of the PACE was substituted with Section 82 of the Criminal Justice and Police Act. The change to legislation meant that a suspect of a crime would have their fingerprints and samples permanently stored on the police national computer (PNC) even after having been acquitted. This paper critically analyses the circumstances of the landmark case of S. AND MARPER V. THE UNITED KINGDOM in two different contexts (i) within relevant domestic law and materials; and (ii) within relevant national and international materials. A comparison is made between the rejection of the application to the Administrative Court on 22 March 2002, a subsequent decision to uphold this ruling by the Court of Appeal on 12 September 2002, and a further dismissal of an appeal by the applicants in the House of Lords on 22 July 2004. This is in direct contrast with a later ruling by the European Court of Human Rights (ECtHR) that was made on 27 February 2008 which in effect rendered Section 82 of the Criminal Justice and Police Act to be in breach of human rights. In closing, the paper considers the reforms instituted by the United Kingdom thus far in response to the ECHR ruling, and their implications on the European Union (EU) at large with respect to elements of the Prüm Treaty.

Keywords: S and Marper v United Kingdom, DNA profiling, DNA sampling, police powers, DNA retention laws, national DNA database (NDNA), European Court of Human Rights, European Convention on Human Rights, proportionality, margin of appreciation, data retention, discrimination, harmonisation, European Union, Prüm Treaty, regulation

1 Background: Who are S. and Marper?

Mr S[1] (the first applicant) and Mr Michael Marper (the second applicant) are both British nationals. Mr S was born in 1989 and Mr Marper in 1963 and both reside in the city of Sheffield. Mr S was arrested on 19 January 2001 when he was only eleven years of age and charged with attempted robbery but about five months later he was acquitted. His fingerprints and DNA samples were taken when he was charged and not destroyed even though he was acquitted of the crime. The police wrote to Mr S's solicitors to inform them that they would retain the samples. The solicitors objected and sought judicial review of that decision. Mr Marper was arrested on 13 March 2001 when he was 38 years of age and charged with harassment of his partner. Before a pre-trial review took place, he and his partner became reconciled, and his partner decided not to press further charges. About three months after he was charged the Crown Prosecution Service decided to formally discontinue the case after serving a notice of intent to the applicant's solicitors. Mr Marper's fingerprints and DNA were also taken and not destroyed after the case was discontinued.[2] Mr Marper's legal team wrote to the South Yorkshire Police[3] requesting the DNA profile be deleted from the NDNAD and fingerprints removed from the Police National Computer (PNC) but the Chief Constable refused the request.[4]

The applicants both applied for judicial review of the police decisions not to destroy the fingerprints and samples. And that is when the more than seven year battle began. Mr S had no previous convictions, police reprimands or warnings, at the time of his arrest and Mr Marper was known to be a person of good character. In both the case of Mr S and Mr Marper the Criminal Justice and Police Act 2001 provided the impetus to retain the fingerprints and profiles indefinitely in relation to a recordable offence,[5] even though both parties were innocent of the respective

1 Mr S's name is never disclosed in the judicial proceedings.

2 Council of Europe, 'Grand Chamber | Case of S. and Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04) Judgment' (European Court of Human Rights, 4 December 2008).

3 'So the reality was that South Yorkshire Police had written a letter to all solicitors saying that because the law had changed they were going to keep all DNA samples of people. In other words they were saying- "[s]top asking for the DNA samples to be destroyed." And then when the email came around and I read this letter, I immediately thought, well that does not really sound right and we should challenge it' (Peter Mahy).

4 Clare Barsby and D.C. Ormerod, 'Evidence: Retention by Police of Fingerprint and DNA Samples of Persons Subject to a Criminal Investigation but not Subsequently Convicted' (2003) January Criminal Law Review 39.

5 B. Hepple, 'The Rights to Privacy and Crime Detection' (2009) 68(2) The Cambridge Law Journal 253.

offences. It must be stated that since the fingerprints and profiles were retained in 2001, U.K. legislation has continued to change surrounding the collection and storage of DNA samples, profiles and fingerprints.[6] In an exclusive interview to *Sky News*, Mr Marper said that the policy which allowed for the retention of a person's DNA sample and profile was just not right. He was quoted:

> 'It was an invasion of privacy, I was offended… They'd taken my rights away and I wasn't going to let them do that… If people get arrested for assault then, yes, their DNA should be taken. But if it goes to court, and it fails, they should be taken off... that way there'll be no innocent people on the database.'[7]

It took Mr S and Mr Marper and the solicitor who represented the applicants, Mr Peter Mahy from Howells LLP on a long journey to the European Court of Human Rights (ECtHR) to finally get the judgment they were hoping for- and in the end a unanimous victory of 17-0 in the Grand Chamber (Figure 1).

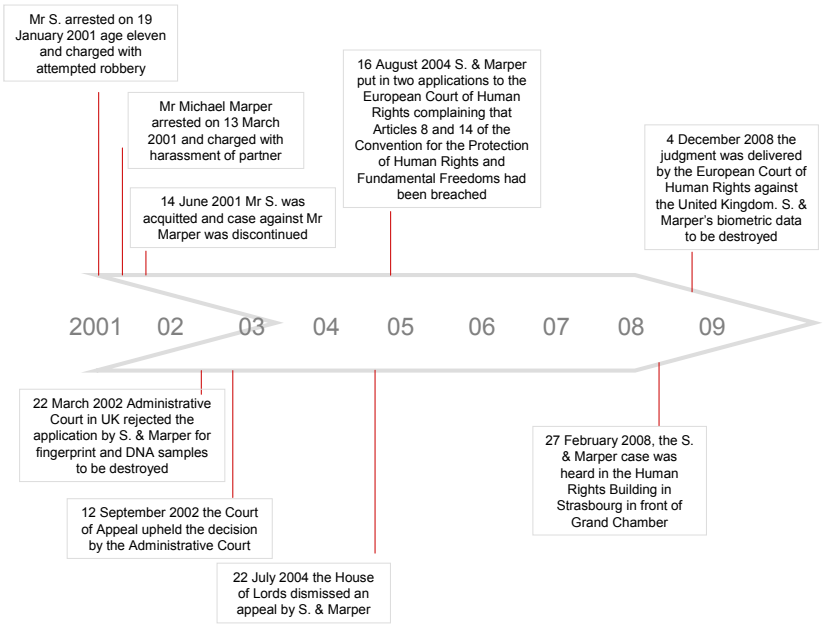


Figure 1: The Road Ahead for Mr S and Mr Marper- All the Way to the ECtHR

6 Ibid 253:'[i]n practice this bioinformation is used speculatively in the investigation of other offences. That was the legislation in force when S and Marper were arrested. Subsequently the Criminal Justice Act 2003 extended police powers even further by allowing the indefinite retention of samples and profiles of those arrested but not necessarily charged with any offence. The Serious and Organised Crime Act 2005 widened the powers of arrest to all recordable offences, however minor.'

7 Mark White, Innocent Names To Be Kept On DNA Database (2009) <http://news.sky.com/skynews/Home/Politics/DNA-Profiles-Of-Innocent-People-To-Be-Kept-On-File-By-UK-Government-For-12-Years/Article/200905115276802> at 20 August 2009.

2 S. and Marper in the U.K. Courts

On the 22nd of March 2002, the Administrative Court rejected the application [[2002] EWHC 478 (Admin)] as ruled by Lord Justice Rose and Justice Leveson. The police refused to destroy the DNA sample and fingerprints of Mr S and Mr Marper. When the applicants appealed the decision to the Court of Appeal, the decision was upheld on the 12th of September 2002, adjudicated by Lord Woolf C.G. and Lord Justice Waller.[8] This left the applicants no other choice than to take their appeal to the House of Lords who on the 22nd of July 2004 dismissed the appeal citing statistical evidence which suggested that some 6 000 DNA profiles had been matched to scenes of crime (SOC) stain profiles.[9]

In commenting on the journey of S and Marper, the solicitor for the applicants, Peter Mahy, noted how the case began with an individual challenge against the U.K. laws. In the Divisional Court and the Court of Appeal, there was little interest by non-government organisations or even the media. Even when the case was heard in the House of Lords, there was relatively no media interest at all. So the case travelled from court to court without much additional physical legal support, save for moral support.

> 'In the Court of Appeal, *Liberty* tried to intervene but they could not come to the hearing. In the House of Lords, again, *Liberty* intervened and they were threatened by the Government that if they did and they came to the hearing there would be costs against them and *Liberty* was fearful of that. So in fact, *Liberty* did not come to the House of Lords. So we were really the only ones against the Police and the Government and we were hugely outgunned' (Peter Mahy).

Despite the claims being made by the applicants on the right to private life, Article 8(1) of the European Convention on Human Rights (ECHR) was probably not even engaged. Art. 8(1) states that everyone has the right to respect for his private and family life, his home and his correspondence.

> 'The feeling in the *U.K.* was very much that this was not a very important issue and why are you here for. And we had a fairly rough ride in the *U.K.* Courts, some even commented that they could not see any basis for the case at all' (Peter Mahy).

The statements made by solicitor Peter Mahy are supported by numerous others analyzing the case at large. In her analysis of the *S and Marper v. United Kingdom* case,

---

8 Hepple, above n 5, 254: 'The Divisional Court (R (on the application of S); R (on the application of Marper v. Chief Constable of South Yorkshire) [2002] EWHC 478 (Admin), [2002] All E.R. (D.) 367) upheld by a majority of the Court of Appeal (Lord Woolf C.J. and Waller L.J.) ([2002] EWCA Civ 1275, [2002] 1 W.L.R. 3233) dismissed applications for judicial review, and the House of Lords ([2004] UKHL 39, [2004] 1 W.L.R. 2196) rejected the appeals.'

9 'DNA and Fingerprints: Indefinite Detention- Prevention and Detection of Crime' (2009) 2 European Human Rights Law Review 260.

Kate Beattie writes:

> '[o]ne of the curiosities of the *U.K.* court judgments in S and Marper was their reluctance to find that retention constituted an interference with art.8 rights at all. Six *U.K.* judges (Rose L.J. and Leveson J. in the Divisional Court and all members of the House of Lords save for Baroness Hale) considered that there was no interference with art.8 or were prepared to acknowledge at most only a very modest interference, seemingly for the purposes of proceeding to the justification analysis under art.8(2).'[10]

Unlike the longstanding United States Fourth Amendment provisions, English law does not have a tradition of privacy protections or mechanisms, despite that it now has a Data Protection Act (1998)[11] and Human Rights Act (1998)[12] in place. The conflict between the judgments by the *U.K.* courts and the ECtHR are as stark as black and white. Beattie emphasizes the point that what the U.K Courts completely ignored, the Grand Chamber considered as vital from the outset- the principle of proportionality was the starting point for Strasbourg.[13] At the heart of the matter in the U.K. courts should have been the foundations of the Data Protection Act spelled out in the definition of "sensitive personal data" and proportionate in relation to the purpose of collection.

2.1 The Administrative Court

One of the major issues raised in the Divisional Court by the legal counsel of Mr S and Mr Marper was the process for removing personal details from the NDNAD and PNC for innocents. As it stood, Peter Mahy made the obvious but important point that the only way innocents could get their details removed from the police databases was by writing a letter to the Chief Constable of the Constabulary where the initial arrest or charges were made.

> 'I think the other major finding was identification from the court that there was no independent system in the *U.K.* for review, and so you have to ask the Chief Constable to remove your DNA and simply that is not fair. That is something that the *U.K.* Government has tried to whitewash a bit, saying that well, we are going to keep that, and the Council of Ministers are saying well that is not good enough. So the finding that you should have the opportunity to have somebody else make the decision was important' (Peter Mahy).

Post the ECtHR judgment Peter Mahy believes that innocent people whose DNA

10 Kate Beattie, 'S and Marper v UK: Privacy, DNA and Crime Prevention' (2009) 2 European Human Rights Law Review 232.

11 Office of Public Sector Information, Data Protection Act 1998 (1998) <http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1> at 5 November 2009.

12 Office of Public Sector Information, Human Rights Act 1998 (1998) <http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1> at 5 November 2009.

13 Beattie, above n 10, 235.

samples and profiles and fingerprints have been obtained are inundating Chief Constables across the U.K. with daily requests to remove their personal details and citizens are certainly voicing and demanding their rights. The S and Marper case challenged the powers of the Chief Constable who only under "exceptional circumstances" and at their own "discretion" could/would remove the details of innocent persons. As has been noted the applications were rejected by the Division Court in March 2002 and the Court of Appeal upheld the judgment by a majority 2:1.

2.2 Court of Appeal

With respect to the Court of Appeal something that is often overlooked is that the Court did find that the retention of DNA samples did interfere with the rights set out in Art. 8(1) but Lord Woolf concluded that the interference was not a significant one given that the personal details of the individual would only be returned given a successful hit in the NDNAD.[14] Thus the risks to a subject's private life, according to the Court of Appeal were of importance between the time the DNA profile was stored in the NDNAD and that time where a successful hit was achieved. But the fact that a successful hit had been achieved to return an individual suspect's DNA profile meant that they might have committed a crime and thus it was a proportionate interference. The Court did not see the indefinite storage of the DNA profile and sample and fingerprints to be a continuing interference with an individual's private life, which might affect the person in a number of different ways, including psychologically, severe inconvenience, lost remuneration, pain, embarrassment etc.[15] The problem with storing personal details of innocents indefinitely is that you are potentially causing indefinite trauma to the individual, a feeling of hopelessness, invasion, loss of dignity, self-confidence and this is a fundamental breach of existing human rights (Art. 11). What good is a clause in an Act, such as the right for an innocent to request the removal of DNA profiles and samples and fingerprints to a Chief Constable, if that discretion is seldom exercised on the premise of making the nation a safer state?

The Administrative Court judgment in the S and Marper case was of no surprise to commentators in the field. In fact, the 'court's deference to the balance struck by Parliament in favour of crime control' was seen by many as predictable but nevertheless a disappointing outcome. The greater inadequacy however probably occurred in the Court of Appeal, when instead of using their own judgment, Lord Woolf C.J and Justice Leveson relied on the conclusion of the Administrative Court reaffirming that the PACE did indeed still strike a balance between the rights of

14 Barsby and Ormerod, above n 4, 39: '[a]lthough the retention of fingerprints and DNA samples interfered with the right of privacy contained in Article 8(1), the adverse consequences to the individual were not out of proportion to the benefits to the public so that there was no defence under Article 8(2).'

15 Andrew Roberts and Nick Taylor, 'Privacy and the DNA Database' (2005) 4 European Human Rights Law Review 385.

the individual and society at large. We might ask ourselves what kind of balance this really is when an innocent person has to have their details stored indefinitely on a national crime information system? What common good is this really achieving? How does it really help society? Surely, it is just impacting on the individual and as Lord Justice Sedley said the individual will "always lose". The idea of "balance" also comes into dispute. Denise Meyerson, plays the devil's advocate, arguing that

> 'instead of balancing rights against the public interest, courts should 'over-enforce' rights, and downgrade the public interest arguments. In effect, this approach would give rights and the public interest different weights from the weight that they would attract on a balancing approach.'[16]

Meyerson claims that we cannot view individual rights and the public interest on the same sliding scale, and when these two claims come head-to-head with one another as competing interests, one must always be considered weightier17 than the other and that Courts should not use their first order reasoning to defend their usual position but consider the problem at hand from the second order reasoning. The decision in the Court of Appeal to uphold the rejection of the S and Marper case in late 2002 did open the floodgates towards the implementation of a compulsory national DNA database. If there was merely a 'moderate' interference with respect to someone's private life, and this interference was proportional based on the public interest, then did it mean that the Government and more specifically the Police, have the power to ask for every single person's DNA and fingerprints and personal information to be stored on the NDNAD, just in case someone offended in the future.[18] According to Peter Mahy, the U.K. '[h]ad always… wanted the largest database possible... [and]… if it was not for the ECtHR ruling, they would have gone for a fully fledged national DNA database.' The second issue stemming from the outcome of the Court of Appeal was that of the future uses (or misuses) and applications that could be based on the DNA samples that were indefinitely stored. These were significant public concerns, especially given the fact that the system

16 Denise Meyerson, 'Why Courts Should Not Balance Rights Against the Public Interest' (2007) 33 Melbourne University Law Review 878.

17 Ibid 879: '[a]ccording to Alexy, when two principles come into conflict, the satisfaction of one must be at the cost of the other and it then becomes necessary to balance the competing interests. He says that in such cases we need to decide which of the principles has more weight on the facts of the case. He understands the concept of proportionality in the narrow sense as demanding such a balancing enquiry, which he sees as requiring a comparison between the 'degree' or 'intensity' of interference with a right and the 'importance' of satisfying the competing consideration. He calls this the 'Law of Balancing', in terms of which, '[t]he greater the degree of non-satisfaction of, or detriment to, one principle, the greater must be the importance of satisfying the other'. Thus, on Alexy's sliding scale approach, the more intensive the restriction, the weightier the reason for restricting it must be.'

18 Roberts and Taylor, above n 15, 391. They reiterated that the outcome of the House of Lords was to strive toward a comprehensive NDNAD, even though this was happening in a haphazard fashion.

was 'devoid of independent organisations safeguarding access, use, research etc.'[19]

2.3 The House of Lords

In the House of Lords the appeal by the applicants was again dismissed. The issue pertaining to Chief Constables' powers came to the fore yet again, when it was concluded by their Lordships that:

> '…a chief constable need not review every case in which samples had been taken from an unconvicted suspect. To do so, it was asserted, "would involve the examination of many thousands of cases and involve large numbers of decision-makers" and consequently "would not confer the benefits of a greatly extended database".'[20]

This response by the Lords was getting to the heart of the matter and signaled to the many observers, including the media, non-government organizations (NGOs) and self-interest groups, that something had to be done about the way in which requests from innocents for the removal of DNA and fingerprint data would be handled. It simply did not make sense that every request could not at least be considered through a standard procedure by an independent review body. The process of involving the Chief Constable was plainly flawed and did not work. But instead of the House of Lords acknowledging this they went on to brush it to the side as an insignificant matter. Post the ECtHR judgment, this has come back to hurt the Constabulary as thousands of U.K. citizens have flocked to exercise their rights.

Again, in the House of Lords, their Lordships stated that they did not consider the retention of DNA samples and fingerprints amounted to an interference with Art. 8. But they did indicate that:

> '[i]f any interference did arise, they considered it a very modest one that could be justified by factors which were proportionate to the legitimate aim in question, including that the information was kept for the limited purpose of the detection, investigation and prosecution of crime.'[21]

The principle of proportionality kept being referred to as the reason why the retention of DNA and fingerprint data could be kept indefinitely, throughout the whole U.K. court journey of S and Marper. But when compared to the statements made by the members of the Grand Chamber at Strasbourg, it is clear that the Lordships in the U.K. were providing a series of argumentation in support of *dis*-proportionality. Furthermore the Lordships rejected the applicants' complaint:

> 'that the retention of their DNA samples and fingerprints subjected them to discriminatory treatment in breach of art.14 when compared to a general body of persons who had not had their fingerprints and samples taken by the police in the course of a criminal investigation.'[22]

---

19 Barsby and Ormerod, above n 4, 40.

20 Roberts and Taylor, above n 15, 391.

21 DNA and Fingerprints, above n 9, 260.

22 Ibid.

3 S. and Marper v. United Kingdom at the ECtHR

In 2005, three years before the ECtHR judgment, Andrew Roberts and Nick Taylor on analyzing the unsatisfactory outcome of the S and Marper case in the House of Lord's predicted to some degree of precision what might happen if the case proceeded to Strasbourg. They pointed out that if the House of Lords' conclusion on Art. 8(1) was to be challenged in Strasbourg and subject to an adverse finding that the domestic analysis on the question of proportionality would come into closer scrutiny.[23] And just as they predicted, the U.K. judgments certainly did come under scrutiny. In the cases of S v. United Kingdom (30562/04) and Marper v. United Kingdom (30566/04), [2008] 25 B.H.R.C. 557, the Grand Chamber of the ECtHR unanimously held that the practice in England, Wales and Northern Ireland of indefinitely retaining fingerprints and DNA samples and profiles of unconvicted persons, without their consent, was a violation of the right to private life guaranteed by Art. 8 of the European Convention on Human Rights (ECHR).[24] The judgment shed light on the limits of police powers in relation to the gathering of personal information for the purposes of crime prevention.[25]

Table 1: Art. 8 and 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11[26]

Article 8 – Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 14 – Prohibition of discrimination
The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Art. 14 as shown in Table 1 was not engaged given that the ECtHR found a violation in Art. 8(2) by the United Kingdom. All in all, the ECtHR focused on the issue of the indefinite retention of a person's DNA and did consider expressly the applicants' 'related criticisms regarding the inadequacy of safeguards surrounding access to their personal data and the insufficient protection against the misuse of such data.' The Court also did not consider it necessary to examine separately the applicants' complaints under Art. 14. The ECtHR judgment is an outcome with incredible

23 Roberts and Taylor, above n 15, 391-2.

24 Hepple, above n 5, 253.

25 Liz Heffernan, 'DNA and Fingerprint Data Retention: S & Marper v United Kingdom' (2009) 34(3) European Law Review 491.

26 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.: 005 (11 April 1950) <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG> at 6 November 2009.

repercussions that will take the U.K. years to comply with properly.

3.1 The Principle of Proportionality and the Margin of Appreciation

For Peter Mahy, the solicitor representing Mr S and Mr Marper, the main findings from the European Court, in direct contrast to the findings of the House of Lords, was Art. 8(2):

> 'what is called the Article 8(2) right, which is the proportionality argument [see Table 10]. They said that they were struck that in the U.K. there was a blanket policy so that everybody's DNA was retained until they were 100 or until they died, no matter who they are or what offence they committed. And they found that the U.K. had overstepped what is called the margin of appreciation, that is the right for each country to determine its own laws and try to strike a fair balance. So all in all, they found that not only was Article 8 (1) engaged but that Article 8(2) on proportionality where states have a lot of lee-way that the *U.K.* had just gone too far and were adopting a blanket one-for-all policy' (Peter Mahy).

In Rasmussen v Denmark, the ECtHR ruled on the scope of the margin of appreciation that it was willing to afford to Member States. It became obvious that some degree of harmonization or common ground had to exist between the laws of the contracting states. But in S and Marper, the laws applicable in England, Wales and Northern Ireland was more an exception than a standard when other states retained DNA samples for crimes of a serious nature, and even then, for a defined period of time.[27] Table 2 shows the author's classification of DNA retention laws in differing states in the Council of Europe (CoE) obtained from the actual judgment.[28] The U.K. was the only state to allow for indefinite retention of DNA samples and profiles, and this even of innocents. As Sir Bob Hepple wrote:

> 'England, Wales and Northern Ireland (but not Scotland) are alone in the 27 EU Member States and also in the 47 Member States of the Council of Europe in retaining indefinitely the DNA profiles and samples of those who have not been convicted of a crime.'[29]

Liz Heffernan in further defining the breadth of the margin of appreciation afforded to national authorities in contracting states identifies important factors that should be considered. These include: (i) the nature of the right, (ii) its importance for the individual, and (iii) the characteristics of the interference and the object pursued.[30] She rightly points out that the margin of appreciation is wider if there is a lack of consensus among the European states. Table 2 clearly shows there is some consensus among contracting states, and that the U.K. is on its own. In addition,

27 Roberts and Taylor, above n 15, 391-2.

28 Council of Europe, above n 2.

29 Hepple, above n 5, 253.

30 Heffernan, above n 25, 497-8.

given the ECtHR was ruling on something of grave importance to the right of the individual, the margin of appreciation was considered narrower. It is possible for instance to hypothesise, that even if the U.K. retained DNA data for 50 years as opposed to indefinitely, this would have still been seen as disproportionate because it was not in line with other contracting states, France being the country that retains the right to keep DNA profiles for 25 years after an acquittal or discharge. The other point to note from Table 2 is that not all contracting member states retain both DNA cellular samples and profiles.

DNA Profile/Sample 'Standards' Category	Council of Europe (CoE) Member State	Period that DNA Profile/Sample Retained
Indefinite Retention	United Kingdom	Permits the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.
Destruction *ex officio*	Belgium, Hungary, Ireland, Italy, Sweden	Require DNA profiles and samples to be destroyed *ex officio* upon acquittal or the discontinuance of the criminal proceedings.
Destruction *ex officio* unless suspicion remains, or person may commit another separate dangerous offence or for lack of criminal accountability	Germany, Luxembourg, the Netherlands	Retention of DNA profiles and samples where suspicions remain about the person or if further investigations are needed in a separate case
	Austria, Poland	Permit retention of DNA profiles and samples where there is a risk that the suspect will commit a dangerous offence/serious crime
	Norway*, Spain	Permit the retention of DNA profiles if the defendant is acquitted for lack of criminal accountability
Destruction *ex officio* after certain period of acquittal or discontinuance	Finland, Denmark	Allow retention for 1 to 10 years respectively in the event of an acquittal
	Switzerland*	Allow retention for 1 year when proceedings have been discontinued
	France	DNA profiles can be retained for 25 years after an acquittal or discharge (during this period the public prosecutor may order their earlier deletion)
	Estonia, Latvia	Appear to allow retention of DNA profiles of suspects for certain periods after acquittal.

* Note: Norway and Switzerland are not EU Member States

Table 2: The ECtHR Ruling on the Margin of Appreciation. The U.K. DNA-related Laws were the Exception between the Contracting States, Not the Norm

In direct conflict with the ECtHR when the House of Lords was asked to consider Art. 8 the right to respect for private life and family life and Art. 14 the prohibition of discrimination, Lord Steyn concluded that:

> 'in respect of retained fingerprints and samples article 8(1) is not engaged. If I am wrong in this view, I would say any interference is very modest indeed' (para. 31)… and that any interference was justified under Art. 8(2) as '... it [was] in the public interest in its fight against crime for the police to have as large a database as possible', with no adverse impacts upon those whose samples were retained.'The retention

> ... does not affect the appellants unless they are implicated in a future crime' (para. 37).

In commenting on Lord Steyn's interpretation of Art. 8(2), Salim Farrar notes cause for concern. He points out that Lord Steyn believes there is interference but qualifies it by his belief that the interference '…is plainly necessary in a democratic society to ensure the investigation and prosecution of serious crime.' Farrar emphasizes in his paper that their Lordships do not consider the principles of proportionality, subsidiarity, accountability and finality, and do not address this principles with respect to Mr S and Mr Marper's individual case.[31] Lord Brown concluded by touting the benefits of an even larger NDNAD (para. 88):

> '... it seems to me that the benefits of the larger database brought about by the now impugned amendment to PACE are so manifest and the objections to it so threadbare that the cause of human rights generally (including the better protection of society against the scourge of crime which dreadfully afflicts the lives of so many of its victims) would inevitably be better served by the database's expansion than by its proposed contraction. The more complete the database, the better the chance of detecting criminals…'[32]

Perhaps the only congruity between the House of Lords and the ECtHR came from Baroness Hale, who dissenting on the issue of DNA indefinite storage, did make the observation that there could be almost nothing more private to the individual than the knowledge of their "genetic makeup."[33] Despite this level of awareness by the Baroness, it was extremely narrow-sighted for her *not* to 'attempt to consider whether the interference with the right to respect for private life was disproportionate in relation to the social benefits.[34] She instead, followed suit with the other Lords, touting the benefits of an expanded database. The ECtHR agreed with Baroness Hale only insofar that 'an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to the determination of the issue whether there has been an interference with the right to private life.'[35] DNA and fingerprint personal data, Roberts and Taylor argue is analogous to a diary in which an individual has catalogued their life story through event descriptions.

> 'If he is compelled to surrender the diary to a third party who then proceeds to read its contents, this would undoubtedly constitute an

31 Salim Farrar, 'DNA Evidence and Human Rights' (2001) 6(1) *Coventry Law Journal* 68.

32 Carole McCartney, 'The DNA Expansion Programme and Criminal Investigation' (2006) 46(2) The British Journal of Criminology 177.

33 Heffernan, above n 25, 495: 'Cellular samples are an abundant source of genetic material and contain highly sensitive personal information about such matters as health and family relationships.

34 Meyerson, above n 16, 896.

35 Hepple, above n 5, 254-5.

> interference with the individual's right to privacy. This will tend to have some inhibiting effect on the way he leads his life.'[36]

Hepple's summation of the House of Lords decision was in relating it to a rather unsophisticated form of utilitarianism, where the embrace of new technologies would herald in a period of optimal social welfare, and where the benefits to the common good would significantly outweigh the costs to the individual. Hepple distinguished between the English judges who perhaps rather lazily relied on age old case law and a utilitarian approach versus the European judges who were very much rights-based and proactive to understand the implications of indefinite DNA storage within the context of today's world.[37] Other differences in the conceptualization of the problem of indefinite DNA storage had to do with the English judges' interpretation of the ECHR. The ECtHR stressed that the European Convention on Human Rights was a

> '"living instrument that must be interpreted in light of present day conditions"; taking into account changing social circumstances and encompassing advances in technology. With this in mind, it is relevant to note that more recent judgments of the European Court disclose an increasing readiness to find that the collection, storage and processing of personal information or data about a suspect interferes with his or her rights under Art. 8(1). [38]

The ECtHR's directive was clear in condemning the U.K. Government (para. 119):

> '[i]n this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed… in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

36 Roberts and Taylor, above n 15, 384.

37 Hepple, above n 5, 255.

38 Roberts and Taylor, above n 15, 378-9.

4 Implications of the ECtHR Judgment

It has been almost 12 months now since the ECtHR judgment was handed down to the United Kingdom. According to Peter Mahy, '[t]he government has been doing as little as possible to comply with the judgment but the Council of Ministers is ensuring that they do comply with the judgment. So although to date, they have been doing as little as they can, in the end they are going to have to comply.' It is interesting to ponder on what compliance actually means in this instance. In actual fact, the ECtHR has the power to award damages to the claimants but the ruling is not automatically binding to the United Kingdom or other contracting states.[39] Thus, there has been some confusion over the impact of the ECtHR judgment on the practices, policies and laws of the United Kingdom, with respect to the indefinite retention of a suspect's personal data, and more widely within the context of the European Union at large.[40]

On the process begun immediately following the ECtHR judgment in December 2008, Peter Mahy commented that it all seemed quite optimistic after the ruling when the then Home Secretary Jacqui Smith MP, said there was going to be a White Paper and that the matter was going to be fully debated with common sense standards. Not soon after that, however,

> '…around about February 2009 time, the Government said they were going to make regulations and secondary legislation so the matter would not be debated. And that is now in jeopardy because the House of Lords Committee said that would be unlawful' (Peter Mahy).

The Home Secretary's exact words were:

> 'We will consult on bringing greater flexibility and fairness into the system by stepping down some individuals over time--a differentiated approach, possibly based on age, or on risk, or on the nature of the offences involved ...The DNA of children under 10--the age of criminal responsibility-- should no longer be held on the database ... and we will take immediate steps to take them off.'[41]

It was also noted by the House of Lords Constitution Committee that primary legislation would replace the regulation with respect the NDNAD that was currently in place which followed an earlier recommendation by the House of Commons

---

39 Christoph Gusy and Sebastian Müller, *How can the Role of the European Court of Human Rights be Enhanced?* (April 2009) JURISTRAS Project <http://www.statewatch.org/news/2009/may/echr-germany-policy-paper.pdf> at 6 November 2009. Gusy and Müller consider the binding force of ECtHR judgments with respect to German law.

40 Adrien Raif-Meyer, Tracey Turner-Tretz and Sania Ivedi, 'Press Release | Grand Chamber Judgment S. and Marper v. The United Kingdom' (Council of Europe, 4 December 2008).

41 Jacqui Smith MP, *Intellect hosts the 'Protecting rights, Protecting society: Balancing privacy and security in the UK' speech by the Home Secretary, the Rt Hon Jacqui Smith video* (16 December 2008) Intellect Technology Association <http://www.intellectuk.org/content/view/4696/462/> at 25 October 2009.

Home Affairs Committee.[42]

This prompted the Government to introduce a three month consultation paper titled *Keeping the Right People on the DNA Database*,[43] on the 7th May of 2009. There were a number of problems related to this consultation paper. First, the Government based their statistics in the consultation on incomplete figures from the Jill Dando Institute, and second the Government provided a very long and very complex document for citizens to understand. Peter Mahy stated:

> 'It is not the sort of document that most members of the public can easily read. It was not in an easy format. There was no sort of response leaflet that had five or six questions that you could answer and send in. There was none of that, no guidance of how to respond. I think for many members of the public that would have been difficult to respond to. We were told that there were however about 500 people that responded. And of course, it was only people who knew about the consultation and could access and understand the document and then just send their response to it' (Peter Mahy).

The Council of Ministers debated the Consultation and U.K. Government proposals on the 15th and 16th of September and there was a resounding consensus amongst the ministers that if the changes were enacted that they would be unlawful.[44] The other problem was that the Consultation was based on flawed statistics which would possibly make the proposed changes unlawful. In October Mahy reflected: 'I think the *U.K.* is in a very difficult position because 10 months on they have not complied with the judgment.'

4.1 Tangible Outcomes

One of the few tangible implications of the S and Marper v United Kingdom case was that both Mr S and Mr Marper had their DNA samples destroyed almost immediately after the ECtHR ruling when a request was made to the South Yorkshire Chief Constable. But unfortunately, this has not meant that innocent peoples' DNA samples collected prior to the ECtHR judgment or during the consultation process

42 Beattie, above n 10, 238. See also the fine work of B. Hepple, 'Forensic databases: implications of the cases of S and Marper' (2009) 49(2) *Medical Science Law* 77 which provides a pioneering summative view of the implications of S. and Marper v United Kingdom. It is limited only in that it is not a historical analysis of the actual implications but speculative in what will happen. It must be noted that Sir Hepple is also the Chair of the Nuffield Bioethics Council.

43 Home Office, *Keeping the right people on the DNA database* (7 May 2009) <http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/> at 6 November 2009.

44 Genewatch UK, *Home Office DNA consultation* (2009) <http://www.genewatch.org/sub-564539> at 22 October 2009: '[t]he proposals in the consultation have been widely criticised for allowing the Government to keep the DNA profiles and fingerprints of innocent people for six to twelve years after they were arrested. Under these plans, people who are rearrested and found innocent again would have to wait another six to twelve years before their database records are deleted.'

(or even after for that matter) have been removed from the NDNAD upon request.[45] According to Mahy what has been happening in the U.K. is:

> '…that the Government, the Home Office, have been telling forces to send a standard letter out to people who have requested destruction of their samples, saying that the law and policy in the *U.K.* has not changed and therefore they would have to wait for a change in the law or policy.[46] And that is what the majority of the people get. And I guess for people who cannot afford to pay privately or eligible for legal aid, they think that that is it, and they do not know any different. We have had quite a lot of clients who have come to us about their situation and we have been challenging it and to date all of our clients DNA samples have been destroyed and taken off but I think the problem is that the majority of people are not fully aware of their rights and are accepting what is said. They do not know how to challenge the government in what they are saying' (Peter Mahy).

There is anecdotal evidence however to suggest that the U.K. police are paying closer attention to individual requests. Following S and Marper, Mark Thomas discussed his situation with a lawyer and a Metropolitan Police Commissioner and the request for his DNA profile to be struck off the NDNAD was fulfilled allegedly with a one line formal letter from the U.K. Police stating: 'I can confirm that a decision has been made to delete your client's fingerprints and DNA sample and DNA profile.'[47] No explanation accompanied this letter.[48] The other issue related to destruction of DNA samples is the determination of a process for which samples to destroy and which to retain.[49] Will it be just those of innocents? Those of innocents under the age of 10 or 18? Or those of low-order recordable offences such as petty crimes that will be eligible to have their stored DNA samples destroyed? And when will

45 Sally Almandras, *Retention of fingerprint and DNA data* (13 May 2009) UK Home Affairs <http://www.parliament.uk/commons/lib/research/briefings/snha-04049.pdf> at 23 June 2009.

46 ACPO, *ACPO comment on consultation of DNA Database* (7 May 2009) <http://www.acpo.police.uk/pressrelease.asp?PR_GUID=%7BB1F9EBA6-432B-45AE-AFCD-F151D621EE1E%7D> at 23 October 2009. In support of Peter Mahy's claims is a statement made by the Association of Chief Police Officers: '[w]e hope this consultation will help to ensure that the police can continue to operate in a lawful, necessary and proportionate manner that is compliant with human rights, while protecting the public from harm. We welcome the opportunity for informed debate in public and parliament on the issues.' That is, that even after the consultation process began, fingerprints and DNA samples continued to be collected as the laws have yet to change in the U.K.

47 Mark Thomas, *How I got my genes deleted* (19 May 2009) The Guardian <http://www.guardian.co.uk/commentisfree/2009/mar/19/dna-database-comment> at 7 November 2009.

48 In contrast to the Mark Thomas case, refer to David Mery, *Three months on, you still can't get off the DNA database: Carry on sampling…* (2 March 2009) The Register <http://www.theregister.co.uk/2009/03/02/dna_dbase_stalling/print.html> at 23 June 2009.

49 Tom Whitehead, *England hangs on to DNA files* (8 May 2009) The Age at 23 June 2009.

this process take place?

While Art. 14 of the ECHR did not come into play during the ECtHR ruling, the legal counsel for Mr S and Mr Marper did rely on *race* and *birth* (i.e. age) issues to bring home their message. The solicitor for S and Marper made the discrimination argument, for instance, that there were more people with ethnic backgrounds on the NDNAD than Caucasians. They also relied on the UN Convention on the Rights of a Child and the European Court certainly saw this as a major issue and especially that children should be entitled to special consideration.[50] But in the end the ECHR did not need to rule on that matter at all, as they ruled on the importance of a right to private life. With respect to the destruction of DNA samples of innocents, Mahy spoke candidly about his personal beliefs:

> 'I am not sure that there is a huge difference… I think that the same rules should apply to everybody. If you are innocent, then it should not really matter what age you are, or what background you are from' (Peter Mahy).

According to Peter Mahy, the current proposals from the Government offer the following guidelines for the retention and deletion of DNA samples and profiles and fingerprints:

> 'For a serious violent, sexual or terrorism related offence, the DNA of a child would be retained for 12 years. For children between the ages of 10 and 18 years who are arrested but not convicted on one occasion, DNA is retained for 6 years then deleted on the 18th birthday, whichever happens first. And if a child is arrested on 2 occasions, their DNA is retained for the full 6 year term. So yes, a different regime for the retention of DNA for children' (Peter Mahy).

4.2 Intangible Outcomes

Another tangible implication of the ECtHR ruling is that the judgment has created change and there is finally a great deal of debate between the parties, in the media, between NGOs, and academics. A comprehensive content analysis of the various stakeholders shows that the *S and Marper v. United Kingdom* case has now received the attention it deserves (Appendix 2); perhaps not S and Marper themselves but what the two gentlemen and their lawyer stood for. Mahy is realistic about what S and Marper really achieved:

> 'I think in a way it has drawn a line in the sand, and hopefully in the next 10-20 years we will look back and say that was an important case. That that was a case, where we took a good look at what was going on in the U.K. and put a stop to the erosion of rights' (Peter Mahy).

50 See also, Cameron A. Price, *DNA Evidence: How Reliable Is It? An Analysis of Issues Which May Affect the Validity and Reliability of DNA Evidence* (1994) 2. Price provides a rich discussion on the rights of a child, and what it means for a child or guardian to consent to a sample being taken.

Mahy's line in the sand metaphor is now resonating in the hearts and minds of civil liberty campaigners, who claimed victory on the 18th of October 2009 'after the government announced it [was] dropping current proposals to retain the DNA profiles of innocent people on the national database.'[51] This being the case, there is still no evidence to suggest when this practice by the police will actually begin and the process it will entail. We know from statistics quoted by the Secretary of State for the Home Department, Mr Alan Campbell, that no more than a total of 255 subject profiles have been removed from the NDNAD between the 9 March 2009 and the 15 October 2009 (Table 3). Table 3 shows the break down of subject profiles that have been removed based on the exceptional case procedure from the NDNAD by U.K. Police Force.[52] With only 40 profiles being removed monthly, it is hard to see at this rate how over 858 000 profiles of innocents will be removed. At this rate it will take the Police and innocent persons till the year 3 796 to remove profiles (1 786 years), and by then the innocents will be deceased anyway which means some profiles of innocents will remain there indefinitely. It seems that only as persons are requesting the deletion of their profiles from the chief officer responsible for a given police force, is the deletion occurring, not via a proactive approach by the Police Force to delete the profiles in one clean sweep. The Commission for Equalities and Human Rights however, is calling for Government ministers to instruct the police to immediately stop taking the DNA of innocent people.[53]

On the optimistic side however, the Home Office has announced that its plans to keep DNA profiles of those arrested (but never convicted) from between six and twelve years depending on the seriousness of the offence have now been dropped from the policing and crime bill currently going through parliament.[54] It has also now been confirmed that that the DNA samples of children under 10 have been removed from the NDNAD but it hard to tell whether these subject profiles have been included in official counts of destruction in Table 3. Mr Alan Johnson has assured Parliament that the NDNAD will from now on be regularly monitored to confirm that this policy remains in effect.[55]

51 Alan Travis, *Home Office climbs down over keeping DNA records on innocent* (19 October 2009) <http://www.guardian.co.uk/politics/2009/oct/19/innocent-dna-database> 22 October 2009.

52 Hampshire Police, *02111 Procedure- Exceptional Case Procedure for Removal of DNA, Fingerprints and PNC Records* (2009) <http://www.hampshire.police.uk/NR/rdonlyres/3253A092-D6D6-48CE-B438-0F24A4A08548/0/02111.pdf> at 25 October 2009.

53 Dayspring, above n 138.

54 Travis, above n 51.

55 Hansard, *DNA Databases* (27 October 2009) <http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091027/text/91027w0019.htm> at 4 November 2009.

Table 3: Number of subject profiles removed from the National DNA Database by each police force from 9 March 2009 to 15 October 2009 (21 Oct 2009: Column 1532W)[56]

U.K. Police Force	9 to 31 March	April	May	June	July	August	September	1 to 15 October
Avon and Somerset	0	3	0	2	0	0	2	0
Bedfordshire	0	0	0	0	2	0	0	0
British Transport Police	0	0	0	1	1	0	0	0
Cambridgeshire	0	0	0	0	0	1	0	0
Cheshire	0	0	0	0	0	0	0	0
City of London	0	0	0	1	0	0	0	0
Cleveland	0	0	1	0	1	1	0	0
Cumbria	0	1	1	2	1	1	1	2
Derbyshire	1	0	0	1	3	8	2	0
Devon and Cornwall	1	1	0	0	1	0	1	0
Dorset	0	1	0	0	1	0	1	0
Durham	0	0	1	0	0	0	1	0
Dyfed Powys	0	0	0	0	0	0	0	0
Essex	0	0	0	0	1	2	1	0
Gloucestershire	0	0	0	0	0	0	0	0
Greater Manchester	1	0	2	0	1	1	0	0
Gwent	0	0	0	0	2	0	0	0
Hampshire	0	0	0	0	2	0	1	0
Hertfordshire	0	0	4	16	4	2	2	0
Humberside	0	0	0	0	0	0	2	0
Kent	0	1	4	2	4	0	5	0
Lancashire	0	0	1	0	0	0	0	0
Leicestershire	0	0	0	0	0	0	0	0
Lincolnshire	0	0	0	0	0	0	0	0
Merseyside	0	0	0	0	0	0	0	2
Metropolitan	5	4	13	7	4	9	10	1
Norfolk	0	0	0	1	0	0	1	0
North Wales	0	0	0	1	0	0	0	0
North Yorkshire	0	0	0	0	0	0	0	1
Northamptonshire	0	0	0	0	0	0	0	0
Northumbria	1	0	0	2	5	1	0	0
Nottinghamshire	0	0	0	0	0	2	3	0
South Wales	0	0	0	0	0	0	2	1
South Yorkshire	0	0	3	0	8	1	0	0
Staffordshire	0	0	0	2	1	1	1	0
Suffolk	0	0	0	0	0	0	0	1
Surrey	1	1	2	2	1	0	0	0
Sussex	0	0	0	1	0	1	0	0
Thames Valley	0	1	1	4	0	1	1	1
Warwickshire	0	0	1	0	0	0	0	0
West Mercia	0	0	1	1	2	0	0	1
West Midlands	0	4	0	1	2	2	5	0
West Yorkshire	3	0	1	0	3	1	1	2
Wiltshire	0	2	0	0	0	0	0	0
Total	**13**	**19**	**36**	**47**	**50**	**35**	**43**	**12**
Grant Total	**255**							

56 Hansard, *DNA: Databases* (21 October 2009) <http://www.parliament.the-stationery-office.co.uk/pa/cm200809/cmhansrd/cm091021/text/91021w0020.htm> at 7 November 2009.

Mahy however, is under no illusion. The S and Marper case was not the end of the DNA controversy in the U.K., but perhaps the very beginning of a new phase in the history of national criminal identification databases for the U.K., Europe and beyond. While the judgment has now well and truly entered the political debate, and the Government will have to shortly respond to the consultation submissions, there will have to be further test cases both from within the U.K. and other contracting members of the ECtHR. In strategizing about the future, Mahy is forward-looking about his plans:

> 'I see the next test case could be somebody who tries to have their DNA destroyed only to be told by the Chief Constable that it cannot. At the moment the Chief Constable is relying on guidelines from 2006 which says the House of Lords ruling is the law. And I think that that is just crazy. The Government is not even taking into account the ECtHR judgment really. I think there would also be an interesting test case on whether it is lawful to take DNA on arrest given that there is no evidential threshold at that stage and I think there is going to be another test case on the issue of keeping DNA for ever and for minor crimes. I think there is going to be lots of test cases as well as the Council of Ministers driving the political debate, so altogether really' (Peter Mahy).

Of the intangible implications of the S and Marper ECtHR judgment one can point to a long list of hopeful outcomes based on proposals submitted to the Home Office during the consultation process by a diverse range of stakeholders. Of the self-interest groups, Genewatch and Liberty have been the most outspoken on the minimal changes that must take place in the U.K. Table 4 is a five point summary of the demands made by Genewatch that are representative of the majority view of most self-interest groups lobbying for socio-ethical issues. These groups do not wish to see the abolishment of the NDNDA but they are very keen that the current laws must be revised and that more public debate is needed to determine the appropriate balance between crime detection, human rights and privacy. Liberty and other such self interest groups welcomed the decision and wished to see the removal of 858 000 profiles of innocents removed from the NDNAD.[57] Genewatch *U.K.* has provided fine details in how individuals should go about requesting the removal of their DNA from the NDNAD calling for all innocents to act:

> '[i]f your DNA is on the database you should now write to the Chief Constable of the police force that arrested you. Ask for them to remove your DNA, fingerprint and police records, and destroy your DNA sample, in the light of the judgment of the European Court of

57 Liberty, *Retaining DNA samples of innocents breaches human rights* (2008) <http://www.liberty-human-rights.org.uk/news-and-events/1-press-releases/2008/04-12-2008-retaining-dna-samples-of-innocents-breaches-human-rights.shtml> at 22 October 2009.

> Human Rights. The judgment applies to anyone who has had charges dropped or been acquitted of a crime. But other cases (e.g. cautions, final warnings, spent minor convictions) may be arguable.'[58]

What is clear from the ECtHR judgment is that the Court was particularly concerned about the risk of stigmatisation and the perception that the applicants were not being treated as innocent, and also about the impact on minors such as Mr S Perhaps we see this most evidently in Mr. S who on 1 August 2009 somehow found his way back onto the NDNAD.[59] What to make of this happenstance? Authorities would have us believe that his DNA profile perhaps should not have been removed from the NDNAD in the first place. But possibly the real answer lies in the ease with which one could find themselves on the NDNAD? Or from a deeper inquiry, Mr S has just lived up to his stigmatization of criminality? Further research inquiry would certainly have to go into the latter. In any case, when asked about Mr S's circumstances, Peter Mahy contented yet again, that in both arrests, DNA was not required in the investigation so it should never have been collected.

Table 4: Proposed Changes Following the *S and Marper v. United Kingdom* ECtHR Judgment- The Majority Representative View of Self-Interest Groups and NGOs [60]

The following are a list of important changes that GeneWatch believe must be made so that privacy and rights safeguards can be made without compromising the use of DNA in fighting crime. These include:

1. A policy of time limits on the retention of people's DNA profiles on the Database, related to the seriousness of the offence and whether a person has been convicted (similar to the original policy adopted when the Database was set up in 1995).
    a. A policy on retention would limit the potential for future governments to misuse the data to restrict people's rights and freedoms. A public debate is needed to establish the details of who should be on the Database and for how long.
2. Destroying individuals' DNA samples once an investigation is complete, after the DNA profiles used for identification have been obtained.
    a. This would limit the potential for personal genetic information to be revealed in future, as science, technology and new policies develop.
3. An end to the practice of allowing companies to undertake controversial genetic research using the Database (which has included attempts to link DNA profiles with ethnicity).
    a. This practice breaches ethical requirements for informed consent to genetic research;
4. A return to the previous policy of taking DNA on charge, rather than arrest, except when the sample is needed to investigate the specific crime for which a person has been arrested.
    a. This would reinstate an important safeguard against the collection of DNA profiles reflecting discriminatory policing;

The creation of an independent, transparent and accountable governing body.'

58 Genewatch UK, *The UK Police National DNA Database* (2009) <http://www.genewatch.org/sub-539478> at 22 October 2009.

59 David Barrett, *Youth who had DNA wiped from database is back on list for drug crime* (1 August 2009) <http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/5955785/Youth-who-had-DNA-wiped-from-database-is-back-on-list-for-drug-crime.html> at 7 November 2009.

60 Genewatch UK, above n 58.

Whatever further outcomes are to be implied by the S and Marper case, time will tell as further provisions on DNA retention will soon be discussed in Parliament on the 18th November when the controversial Policing and Crime Bill will be under scrutiny.[61] Clause 96 of this Bill proposes to insert new sections into the PACE '… which would enable the Secretary of State to make regulations about the retention, use and destruction of material—including photographs, fingerprints, footwear impressions, DNA samples and information derived from DNA samples.'[62] The House of Lords considered the question of retention of samples gathered during police investigations in the course of an inquiry into the constitutional framework governing surveillance[63] and concluded that

> '... DNA profiles should only be retained on the National DNA Database (NDNAD) where it can be shown that such retention is justified or deserved. We expect the Government to comply fully, and as soon as possible, with the judgment of the European Court of Human Rights in the case of S and Marper v. the United Kingdom, and to ensure that the DNA profiles of people arrested for, or charged with, a recordable offence but not subsequently convicted are not retained on the NDNAD for an unlimited period of time.'[64]

The House of Lords also believe that law enforcement authorities should improve the transparency of consent procedures and forms when adding DNA profiles to the NDNAD. Another refreshing move was toward the removal of volunteer profiles from the NDNAD, in such cases where mass screenings have taken place in the past, unless volunteers explicitly consent to the retention.[65] In contrast, the view of most NGOs, would be to see the removal of volunteer DNA profiles completely from the NDNAD so as to reduce the chance of false hits.

The House of Lords also expressed concern that the NDNAD is currently not government by a single statute. The view of their Lordships is that the NDNAD would be better served by a Government bill to replace the existing regulatory framework, which would allow for a fresh debate over the rules pertaining to the length of time for which DNA profiles are retained.[66] This is a perfect opportunity for this new bill as the public consultation process is now complete and further

---

61 House of Lords, *Policing and Crime Bill - Constitution Committee Contents* (2009) <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/128/12803.htm> at 7 November 2009.

62 Ibid.

63 House of Lords Select Committee on the Constitution, 'Surveillance: Citizens and the State (Vol 1 Report)' (House of Lords, 2008-09). See also, Lord Chancellor and Secretary of State for Justice, 'Government Response to the House of Lords Select Committee on the Constitution's Report Surveillance: Citizens And The State' (The Stationary Office, 2009).

64 House of Lords, above n 61.

65 Ibid.

66 Ibid.

research could be grounded in this primary data from a variety of stakeholders.[67] As for the Policing and Crime Bill, if the proposed Clause 96 was to be agreed upon, it would have devastating repercussions for NDNAD reforms and would not allow for parliamentary oversight and debate to occur. The House of Lords is calling for the Government to think about its policing policies again, and to 'bring forward proposals in a separate bill to regulate the National DNA Database.'[68]

4.3 Towards a Harmonization of DNA-related Retention Laws in Europe

The Grand Chamber judgment has forced a belated reconsideration of the overgrown NDNAD and DNA retention laws in England, Wales and Northern Ireland.[69] In this instance, rather than looking at models of retention abroad, the U.K. could look to align with Scotland. Beyond the implications of S and Marper in the U.K. however, we must also look at what the judgment means for the Council of Europe member states. The Grand Chamber of the ECtHR was sending a clear message to national authorities abroad,[70] and not just with respect to the collection and storage of DNA samples and profiles but also of fingerprint data in criminal identification applications. Fingerprint data because it cannot divulge sensitive genetic-based information has been somewhat ignored by the media and even the self-interest groups. This may have something to do with the widespread use of fingerprints today for international travel in electronic passports etc. Even Peter Mahy commented:

> 'I do not see fingerprints as being as big an issue as DNA. I think with DNA it is the fear of future uses that worries people and people do not understand exactly what DNA is and what it could be used for. Whereas fingerprints are seen more as a signature and that less pieces could be extracted from it. But I think generally, especially with my clients, they are less concerned about fingerprints or a photograph than they are about DNA' (Peter Mahy).

But even so, the onus is now back on the member states to provide adequate proof of their personal data collection regimes as being proportionate to the need to reduce crime.

Inevitably such realignment of DNA regulations and laws would have

67 Travis, above n 51.

68 House of Lords, above n 61.

69 Beattie, above n 10, 230.

70 Heffernan, above n 25, 503: '…given the range and diversity of European state practice, other governments are also on notice of the need to ensure that they meet the rigorous standards for the protection of personal information set down by the Court. By setting a relatively low threshold for an interference with the right to respect for private life under Art.8 para.1, the Court has placed the onus squarely on national authorities to monitor compliance with the Convention and justify any encroachment as proportionate to society's interest in the prevention of disorder and crime.'

repercussions on new treaties, such as the European Union's Prüm Treaty of 2005 which allows for the sharing of DNA data, fingerprint and vehicle registration data for the purpose of countering acts of terror and bringing criminals to prosecution. The Prüm Treaty was a German-led initiative to increase cross-border cooperation for the combating of terrorism, crime and illegal immigration.[71] The Agreement was hastily[72] signed raising fundamental questions over the main provisions of the Treaty which focused on reciprocal access of Member States to national databases containing biometric data (such as DNA profiles and fingerprints), and vehicle registration data.[73] Despite, little time being dedicated to debating the contents of the Agreement, by June 2007 the provisions had found their way into the legislative framework of the European Union.[74] Even the United Kingdom[75] reluctantly signed the Convention. In provisions in Chapter 2 of the Prüm Treaty, it is written that contracting parties must ensure both availability and access to data such as DNA identifiers through automated online searches. Art. 2(1) states that: 'Contracting Parties shall ensure the availability of reference data from their national DNA analysis files' and that '[r]eference data shall only include DNA profiles established from the non-coding part of DNA and a reference.' It is clear that the reference data must not contain any information that can identify the subject but it still does build on a great number of attributes (compare for instance the Schengen Information System (SIS) dataset with the Prüm Treaty additional attributes in Table 5). What implications does this have for the *U.K.* NDNAD? If the DNA profiles of innocents continue to be stored on the NDNAD, then it is quite possible that the risk associated with a false hit on these profiles is not merely, national, but now European Union-wide.

---

71 Council of the European Union, *Prüm Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration* (7 July 2005) <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf> at 22 June 2009.

72 Franziska Boehm, *Confusing Fundamental Rights Protection in Europe: Loopholes in European Fundamental Rights Protection Exemplified on European Data Protection Rules* (24 February 2009) University of Luxembourg Law Working Paper No. 2009-01 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1348472> at 24 June 2009. See also, Cillian Donnelly, *Prüm could still become European law despite reservations* (7 May 2007) <http://www.eureporter.co.uk/prould-still-become-european-law-politics-archive-102364.html> at 24 June 2009.

73 Justice and Home Affairs, *Prüm Treaty will allow EU27 to exchange DNA data to fight crime* (7 June 2007) European Parliament <http://www.europarl.europa.eu/sides/getDoc.do?language=EN&type=IM-PRESS&reference=20070606IPR07542> at 23 June 2009.

74 EUROPA, *The Integration of the "Prüm Treaty" into EU-legislation - Council decision on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime* (12 June 2007) <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803> at 23 June 2009.

75 European Digital Rights, *Prüm's Treaty is now included into the EU legal framework* (20 June 2007) <http://www.edri.org/edrigram/number5.12/prum-treaty-eu> at 23 June 2009.

Table 5: Personal and Biometric Data Collected of Criminals Stored on the SIS and Prüm Treaty Mechanism that can now be Shared between Contracting Parties of the EU

Schengen Information System (SIS) Data	Prüm Treaty Data Additions
Person-specific Data: Surnames, aliases, physical characteristics not subject to change, date and place of birth, sex, nationality, whether persons concerned are armed or violent, reason for alert, action to be taken *Object/Vehicle-specific Data:* Stolen motor vehicles, firearms which have been misappropriated, blank official documents which have been stolen, issues identity papers which have been stolen and suspect banknotes.	*Person-specific Data:* Biometric data including DNA and fingerprint (dactyloscopic) data identification patterns *Cross-border Flows:* Cross-border access to data subject to the principle of availability *Hot Pursuit:* In urgent situations, officers from one Contracting Party may, without another Contracting Party's prior consent, cross the border so that they can take provisional measures necessary to avert imminent danger to the physical integrity of people.

5 Conclusion

Reflecting on the complexity of changes to national laws and supranational laws and these contending with conflicting conventions at the EU and CoE levels, we can only come to the conclusion that the road ahead will be increasingly challenging for law enforcement agencies, governments, and citizens in the EU especially. If S and Marper achieved anything of long-standing acclaim, it was in the words of Liz Heffernan, a

> 'tightening in the governance of the flourishing phenomenon of criminal databasing across Europe… S and Marper v United Kingdom is a telling reminder that a careful watch must be maintained to ensure that the gradual extension of databasing programmes, with associated increases in police powers, does not infringe protected rights and freedoms.'[76]

The ECtHR highlighted the major responsibility placed on nations like the U.K. and the U.S. who are leading in the development of new technologies and innovations as applied to crime. What is clear from our experience of fingerprints is that if we do not protect the rights of citizens from the encroachment of biometrics (including DNA) in applications like border control, or other aspects of social life such as

76 Heffernan, above n 25, 503-4.

employment and health insurance,[77] then we will almost certainly find ourselves living in a world portrayed in the realms of *Gattaca*.[78] For Heffernan, this is not just an accidental occurrence, it is technological intervention creeping into social life, 'gradually, incrementally, but deliberately, increased over time.'[79] The concept is not new in the field of information systems development. The idea is known as "function creep", the way in which information that has been collected for one limited purpose is gradually allowed to be used for other purposes which people may not approve.[80] And it is here where the interplay between science, law and society will inevitably see a great deal of new research being conducted.[81]

77 Price, above n 29, 39. 'There is growing concern in the USA about the intrusive requests by employers and insurance companies for DNA tests as a prerequisite for one to be hired or insured. The rationale for the requests is based on the financial risks that are assumed by both employers and insurance companies, both often in the field of pension benefits. Insurance companies have always been entitled to require applicants to undergo medical tests before an insurance proposal is accepted, accepted with conditions, or declined. Some of their newer medical questions over the last ten years have been directed at lifestyle habits which could indicate an increased likelihood of exposure to AIDS. Because premiums are calculated actuarially from life expectation tables, any undue exposure to high risks reflects in increased premiums, or lower bonuses, for all policy holders. Consequently there has been only muted objection to the direction taken by insurance medical questionnaires.'

78 Andrew Nicol, *Gattaca* (1997). See also, Kirk W. Junker, 'Gattaca: defacing the future' (1999) 31(6) *Futures* 631.

79 Liz Heffernan, 'Genetic Policing: The Use of DNA in Criminal Investigations by Robin Williams and Paul Johnson (Willan Publishing, 2008)' (2008) (48) *British Journal of Criminology* 700.

80 OUP, *Function Creep* (2009) Oxford University Press <http://www.oup.com/elt/catalogue/teachersites/oald7/wotm/wotm_archive/function_creep?cc=global> at 7 November 2009.

81 Johanne Yttri Dahl and Ann Rudinow Sætnan, '"It all happened so slowly" – On controlling function creep in forensic DNA databases' (2009) 37(3) *International Journal of Law, Crime and Justice* 83.

14

An Interview with Mr Peter Mahy of Howells LLP who represented S and Marper at the European Court of Human Rights

Katina Michael[1] with Peter Mahy[2]

[1]University of Wollongong, [2]Howells LLP

Abstract

Mr Peter Mahy, Partner at Howells LLP and the lawyer who represented S & Marper in front of the Grand Chamber at the European Court of Human Rights was interviewed by Katina Michael on the 10th of October 2009 while she was studying towards a Masters of Transnational Crime Prevention in the Faculty of Law at the University of Wollongong. In 2010 Peter Mahy received the Legal Aid Lawyer of the Year award for his contribution to the field. Mahy received his honours law degree from Sheffield University and a Masters in Criminology from the University of Cambridge. He did his Legal Practice Course at the University of Northumbria, Newcastle and joined Howells in 1996, qualifying in 1998.

Keywords: S & Marper v United Kingdom, European Court of Human Rights, DNA, national database, proportionality, government, police, citizens

Katina Michael: Peter, thank you for the opportunity to conduct this interview with you. I will begin by asking you to distinguish between the collection and storage of DNA samples as opposed to DNA profiles? Or do you see both collection types are 'equal' in value?

Peter Mahy: I do distinguish between DNA sampling and DNA profiling. And in fact, the UK government is now also distinguishing between DNA samples and profiling, stating in their consultation paper, *Keeping the right people on the DNA database,* that samples will be destroyed. I think there is a particular distinction in that there is a fear with how samples may be used in the future, and how they might be analysed into the future. However to me personally, I think the collection and storage of DNA profiles as opposed to DNA samples is marginal and that both are of a huge concern.

Katina Michael: So the UK government has now publicly stated that they will destroy all samples on their national database?

Peter Mahy: Yes. So what they are saying now is that the DNA sample will be destroyed once it has been uploaded to a profile.

Katina Michael: Could you make a general comment about the British Police and Criminal Evidence (PACE) Act 1984 and how it has changed since its introduction?

Peter Mahy: So prior to 2001, the UK took the position that if you had your DNA taken on charge then it could be kept but if you were acquitted or the charge was not continued then it had to be destroyed. That was changed in 2001, so that DNA could be retained even after acquittal or if charges were dropped. And then the law again changed so that a DNA sample could be taken just on arrest, not charge. So the PACE in terms of the collection of DNA was significantly watered down.

Katina Michael: Is it true that PACE has been watered down so much that it has been applied to the collection of DNA samples for what society generally considers petty misdeeds? Was DNA collected first for violent crimes alone, and then later due to changes in PACE for minor misdemeanors?

Peter Mahy: So what has happened now, is about police powers with respect to recordable offences. And so every 6-12 months, the notion of what constitutes a recordable offence is redefined, and each time it gets redefined more offences are introduced into PACE, including more lower level crimes. So there has been a widening of the definition on what constitutes a recordable offence, to include more minor offences.

Katina Michael: Some analysts, early on (e.g. Ireland 1989) have argued that PACE did a good job of balancing the right of an accused person against the need for police to have adequate powers for law enforcement. Do you agree?

Peter Mahy: I think the problem in the UK is that you see an increasing amount of criminal legislation. There has been 3000 changes to acts of parliament related to criminal legislation since the Labour government has been in, so there has been a creep to the erosion of civil liberties, a hemming in if you like, and so it seems to be a constant battle to keep the rights that were enshrined in PACE and the

Human Rights Act.

Katina Michael: Do you see then, that the increase in police authority and powers represents a commensurate loss in the individual rights of UK citizens?

Peter Mahy: So I think there is sort of a constant creep against civil liberties, and a constant battle to preserve them. And it is not clear cut. The UK enacted the Human Rights Act which was a massive step forward but that is under threat at the moment. There is a conservative party here that is saying they are going to take away the Human Rights Act. This could be seen a battle between the left and right all the time, trying to keep the rights that have been hard fought for.

Katina Michael: As a solicitor representing persons in cases to do with civil liberties, how do you feel about the collection of DNA samples for crimes such as: petty misdeeds such as begging, or being under the influence of alcohol, and acting in a disorderly fashion?

Peter Mahy: I think an interesting issue in this whole case and this whole debate is that no one has really grappled with why DNA has been taken from a person at all. If a person is presumed innocent, I mean, why should you take their DNA on arrest or on charge? That lead into the question really. Is it right to take the DNA of a person for very low level offences? I think that no one has really grappled with this, of when do you draw the line and when should it be taken?

Katina Michael: I agree. I am actually interested in this very question. And perhaps more specifically I am interested in why more citizens do not speak up about the collection and long term storage of their DNA samples and profiles. Is it that citizens feel powerless? Or that they do not know how to fully participate in such a process of questioning?

Peter Mahy: I think that what has been absolutely amazing in this case is that when this case started out it was pretty much just me challenging the law. There was so little interest in the divisional courts, little interest in the Court of Appeal. Even at the House of Lords, the media was not really interested, not at all, so there was really no profile. When we got called from the European Court of Human Rights things began to get a little bit more exciting. And then there was the Nuffield report that was big publicity. And after the European Court there seems to be something on DNA in the press every day, and I think now it has a high profile. When you listen to documentaries on television here, or question time which is very popular, there is just about something on this every week because this really is a big issue now and it has come as a result of the stand that we took. And it seems that this *is* a major issue. In terms of people challenging government and taking it forward– I understand that Chief Constables are virtually inundated with daily requests at the moment and citizens voicing and demanding their rights.

Katina Michael: That is great to hear. And I do hope it sets an example for others to follow, causing a ripple effect through the Europe, and the rest of the world. Does the UK government actually have about 9% of all UK citizen DNA samples?

Peter Mahy: Yes it does. The figures that we have over here are that there are just

over 5 million samples on the DNA database with about a 60 million population in the UK, so it is roughly between 8%-9%. I mean it is a particular problem here because these are the statistics that we have been given over the years by the Government, but they seem to change a lot and are quite unreliable, and that is one of the key problems. So I am rather skeptical about the UK figures that they are putting forward but it seems to be around the 5 million mark.

Katina Michael: So when you compare the percentage of the UK population that has had their DNA sample stored (about 9%) on the national DNA database with other countries in the world (about 2%) do you believe that the collection is 'grossly disproportionate'? Are we to believe that crime rates are so high in the UK, or there are other historical reasons to describe this kind of sampling?

Peter Mahy: I think the UK in the last few years has become fairly obsessed with crime and it has been a policy of the government to focus on this. And the government was particularly proud in this case to say that they were the vanguard of DNA and of the biggest database and therefore they would be able to conduct crime detection but without really thinking about the implications. So it was actually the Government who wanted to have the biggest database. I think the government also saw it as a cheap way of fighting crime, and cutting costs and trying to keep the public happy.

Katina Michael: And are the retention laws in the UK, post S & Marper bound to change?

Peter Mahy: This is quite a difficult question. The government has been doing as little as possible to comply with the judgment but the Council of Ministers is ensuring that they do comply with the judgment. So although to date, they have been doing as little as they can, in the end they are going to have to comply.

Katina Michael: Could you elaborate on the main issue the ECtHR case identified which was to do with the principle of "proportionality" and an individual's right to respect for private life? Was this the key finding? What were some of the other findings from your viewpoint?

Peter Mahy: I think one of the important things to realise is that in the UK courts, we traveled from the Divisional Court, the Court of Appeal, and the House of Lords, and while in the UK it was stated that Article 8(1) the 'right to private life' was probably not even engaged. The feeling in the UK was very much that this was not a very important issue and why are you here for. And we had a fairly rough ride in the UK courts, some even commented that they could not see any basis for the case at all. In the ECtHR, they said clearly that article 8(1) was engaged and that was an important finding, from the UK point of view certainly that these rights have to be taken seriously. I think the other major finding was identification from the court that there was no independent system in the UK for review, and so you have to ask the Chief Constable to remove your DNA and simply that is not fair. That is something that the UK Government has tried to whitewash a bit, saying that well, we are going to keep that, and the Council of Ministers are saying

well that is not good enough. So the finding that you should have the opportunity to have somebody else make the decision was important. But the main findings from the European Court were what is called the Article 8(2) right, which is the proportionality argument. They said that they were struck that in the UK there was a blanket policy so that everybody's DNA was retained until they were 100 or until they died, no matter who they are or what offence they committed. And they found that the UK had overstepped what is called the margin of appreciation, that is the right for each country to determine its own laws and try to strike a fair balance. So all in all, they found that not only was Article 8 (1) engaged but that Article 8(2) on proportionality where states have a lot of lee-way that the UK had just gone too far and were adopting a blanket one-for-all policy.

Katina Michael: How do you think the United Kingdom have reacted to the ECtHR ruling? And have they reacted enough and at the required speed?

Peter Mahy: What happened in December 2008 the Home Secretary, who has of course now been chucked out, said there was going to be a white paper and that the matter was going to be fully debated with common sense standards. Not soon after that, around about February 2009 time, the Government said they were going to make regulations and secondary legislation so the matter would not be debated. And that is now in jeopardy because the House of Lords Committee said that would be an unlawful. The Government then introduced the consultation paper, *Keeping the right people on the DNA database,* in May of this year, and importantly, based their statistics from the Jill Dando Institute. The Jill Dando Institute recently said that the statistics that the consultation is based on were not finished. So that puts the whole consultation up in the air. And most importantly the Council of Ministers debated this on the 15th and 16th of September this year, and looked at the UK proposals and they basically said that for most of them that if they were enacted, then they would be unlawful. So I think the UK is in a very difficult position because 10 months on they have not complied with the judgment. And that they have put proposals forward that are based on flawed statistics and which the Council of Ministers have said would probably be unlawful.

Katina Michael: And you have mentioned the citizen response has been to inundate the Chief Constables with requests to remove DNA samples. How have you felt about the consultative process as of May 2009?

Peter Mahy: Part of the problem with the consultation process from my point of view, is that for a public consultation the Government provided a very long and a very complex document. It is not the sort of document that most members of the public can easily read. It was not in an easy format. There was no sort of response leaflet that had five or six questions that you could answer and send in. There was none of that, no guidance of how to respond. I think for many members of the public that would have been difficult to respond to. We were told that there were however about 500 people that responded. And of course, it was only people who knew about the consultation and could access and understand the document and

then just send their response to it.

Katina Michael: So S & Marper's DNA samples were removed after the ECtHR ruling? And what about the samples of other innocents? Were they destroyed or are they still on the database?

Peter Mahy: Our clients' samples were destroyed in December 2008, almost immediately after we requested destruction, after the ECtHR ruling. What has been happening in the UK is that the Government, the Home Office, have been telling forces to send a standard letter out to people who have requested destruction of their samples, saying that the law and policy in the UK has not changed and therefore they would have to wait for a change in the law or policy. And that is what the majority of the people get. And I guess for people who cannot afford to pay privately or eligible for legal aid, they think that that is it, and they do not know any different. We have had quite a lot of clients who have come to us about their situation and we have been challenging it and to date all of our clients DNA samples have been destroyed and taken off but I think the problem is that the majority of people are not fully aware of their rights and are accepting what is said. They do not know how to challenge the government in what they are saying.

Katina Michael: What is the next step in this process? What will it take for the UK Government to destroy the samples?

Peter Mahy: The Labour Government here is very reluctant and I think in truth that they are hoping that this issue is just going to go away before the general election which is scheduled for the next six months or so. I am skeptical that they are going to do anything before then but they have Europe on their back and the Conservative Government which is interestingly seen as more right wing has said that they will comply with the ECtHR judgment, and will destroy the DNA samples of all innocents as will the Liberal Democrat Party. So it all depends on who is in power. But I think either way eventually the UK is going to have to comply with the judgment and destroy DNA samples of innocents or at least have a fairly limited retention period as they do in Scotland.

Katina Michael: Do you wish to comment about reports in the media that Mr S has somehow found his way back onto the DNA 'archive'? Authorities would have us believe that Mr S's details should never have been removed from the National DNA Database (NDNA) in the first place, but is the real story more about the 'ease' with which one's DNA sample can end up on the NDNA?

Peter Mahy: I think in a way it is the Government trying to make the most of it, but it is a false premise really, because the point is that Mr S was arrested again, and his DNA was put back on the NDNA. But they did not need his DNA to get there, i.e., it made no difference that his DNA was taken off in the first place. As I understand it, DNA was not involved in either of the cases at all. In fact, DNA was not a feature of either case, so it would not have made any difference at all.

Katina Michael: So your response is basically, what is the point of collecting and storing DNA when it cannot add any value to the actual case in question?

Peter Mahy: Yes, in the case of our client, what did it matter, DNA played no part at all.

Katina Michael: So why have the UK adopted such a stance? Are they attempting to make their statistical inferences more robust when DNA is being analysed in criminal proceedings?

Peter Mahy: Certainly the UK's policy has always been that they have wanted the largest database possible. I think if it was not for the ECtHR ruling, they would have gone for a fully fledged national DNA database.

Katina Michael: So I gather from my reading that the motivation for such a national DNA database has to do with providing a greater probability and confidence level between the DNA evidence found at the scene of a crime and a match with the DNA sample of a suspect and to eliminate such problems linked to the need to conduct sub-group sampling?

Peter Mahy: Many of the commentators now- and this is where we are getting into more scientific discussion and more areas of argument- are saying that they consider four to five million samples to be the largest for an accurate DNA database. And that if your database size goes over five million that your chances of getting false hits and false readings increase. I was reading one article that was discussing how the chances of false hits is now increasing as a result of increasing records on the NDNA.

Katina Michael: What do you think the 'Father of DNA' thinks about all this?

Peter Mahy: Well in fact, Alec Jeffreys has gone on record over the last few years saying that the DNA samples of innocents should not be kept and should be destroyed.

Katina Michael: Could you make a comment about the collection of DNA samples from:

a) Children?
b) Persons under the age of 18?
c) Or of particular ethnic/racial/familial backgrounds

and what impact this might have in a court of law?

Peter Mahy: This was something we relied on the UN Convention on the Rights of the Child and the European Court certainly saw that as a big issue, and that children are entitled to special consideration. And we also made the discrimination argument that there are so many more people of ethnic backgrounds than Caucasians as well. But in the end the ECtHR did not need to rule on that matter at all, as they ruled on the importance of a right to private life. Personally, I am not sure that there is a huge difference, and personally I think that the same rules should apply to everybody. If you are innocent, then it should not really matter what age you are, or what background you are from.

Katina Michael: So how is the Government proposing to change DNA retention laws by age and type of offence?

Peter Mahy: So there are proposals from the Government to that end. For a serious

violent, sexual or terrorism-related offence, the DNA of a child would be retained for 12 years. For children between the ages of 10 and 18 years who are arrested but not convicted on one occasion, DNA is retained for 6 years then deleted on the 18th birthday, whichever happens first. And if a child is arrested on 2 occasions, their DNA is retained for the full 6 year term. So yes, a different regime for the retention of DNA for children.

Katina Michael: What would it take to raise the profile of the importance of removing DNA samples from public databases, especially in the European Union or Council of Europe states? Will it take more cases like S & Marper to front up to the ECtHR or various EU states to remove samples from databases? What strategy would you adopt?

Peter Mahy: I think we now have the judgment and it is now in the political debate and the Government will have to respond to the consultation submissions shortly. And after the ECtHR judgment the Government has been under constant pressure. There will be more test cases from people like me. I see the next test case could be somebody who tries to have their DNA destroyed only to be told by the Chief Constable that it cannot. At the moment the Chief Constable is relying on guidelines from 2006 which says the House of Lords ruling is the law. And I think that that is just crazy. The Government is not even taking into account the ECtHR judgment really. I think there would also be an interesting test case on whether it is lawful to take DNA on arrest given that there is no evidential threshold at that stage and I think there is going to be another test case on the issue of keeping DNA for ever and for minor crimes. I think there is going to be lots of test cases as well as the Council of Ministers driving the political debate, so altogether really.

Katina Michael: Could you make a comment on the collection and exchange of DNA data as a result of the Prüm Treaty? Do you see this as magnifying the problem of collecting DNA samples of innocents and those acquitted?

Peter Mahy: To be honest, we never got to the bottom of how this works in practice. For instance, if someone has there DNA sample taken in the UK and a DNA profile is exchanged between EU states and then a request for deletion is made and granted in the UK, who knows where your information has been saved? Has it been saved in different places all around the world? I am not sure even the Government has a handle on what they have been doing with this information.

Katina Michael: Yes the loss of information is a critical issue for such sensitive databases.

Peter Mahy: I do not know if you heard but in the UK last year, there was a database of DNA profiles with known sex offenders sent from the Dutch police to the UK). Somehow the disc was misplaced and found over a year later. There has been a whole history here in the UK of data going missing, including prison inmate details, bank account details etc. The point is that mishandling of such information is possible. The matter seems to have gone quiet now but this seems to be a huge issue. It seems to me however that there are even more fundamental issues. Say for

instance we are sharing DNA profiles with country X who is currently considered our 'friend' and then 10-20 years down the track they become our 'enemy'. This then becomes a serious terrorist threat. These DNA samples and profiles can then be used against us and to cause huge threat against us.

Katina Michael: Given my background is in information technology, I do read so many articles on the losses of data such as disks left behind at train stations and airports, unencrypted data being intercepted, and the theft of laptops of very important persons. But I really had not gone to that next step to consider the way in which DNA profile data in particular, could be used to attack and to make the most of a potential terrorist act. That is fascinating-

Peter Mahy: Yes, it is pretty scary… You could just imagine that even on 5 million samples in the UK getting into the wrong hands and from those records you could determine which type of chemical or biological warfare could wipe out 90% of the UK population but would allow other states to be somewhat unaffected. There would be a significant danger.

Katina Michael: When government authorities quote statistics related to the number of cold cases solved using DNA evidence/samples, or the number of successful convictions based on the process of matching DNA profiles, are we really to believe them?

Peter Mahy: Well, again, the government statistics are extremely unreliable. I think an important thing to note is that from the Council of Ministers discussion a couple of weeks ago, the information they have actually been given from the Government themselves is that of the 850000 or so samples that are potentially from innocent people that 350000 are from people who have been convicted or acquitted. And from those 500000 samples that are left they do not know what happened to those individuals. So when you have a database with 10% of samples of which the Government has no idea of whether those people were convicted or innocent then I think that just shows how very statistically unreliable the data sources are.

Katina Michael: I would like you to comment on the use of force in obtaining intimate and non-intimate DNA samples without the suspect's consent? What does 'refusal without good cause' actually mean in the United Kingdom with respect to PACE? Do you know of any cases where this has occurred and innocent person has not been incriminated? The exact phrase that is used in s. 62(10) is: "Where the consent by the detained person is refused without 'good cause', the court, and the court and jury, may draw inferences that may amount to corroboration of any evidence against the person in relation to the refusal s. 62(10)."

Peter Mahy: I can answer that in a slightly different way using an example of a case that I recently dealt with where I had a very well respected client in the community, who with his wife was arrested for stealing their own car. At the police station they were asked for their DNA sample and they refused and it was taken by force. We have been battling to get that DNA destroyed for 2 years or so, and only post Marper and only recently, in fact only in the last month or two, we finally got it destroyed.

And to those people I think that the whole way it was approached by the police initially in taking the DNA sample by force from somebody who clearly had not committed an offense and who were not charged at the police station and were let go after that, simply to boost the number of people in the database, is horrific and unnecessary. And the battle for 2 years after, alienates people and I think that is why the Government has gone wrong on this issue because you should be policing by consent rather than by coercion. Those two clients before this ordeal were engaged helping the police and very appropriately will now be very reluctant to help the police and there are hundreds of thousands of other people who feel the same way.

Katina Michael: Perhaps it is a good time now to ask you about initiatives such as the Innocence Project in the United States (1992) and the Innocence Network in the United Kingdom (2004). Do you believe that increasingly DNA evidence is rightly being used as a critical component of many judicial proceedings? Or do you think it is being overused? That is, DNA evidence can be used to both inculpate and exculpate a suspect; that DNA evidence has the power to convict the guilty or exonerate the innocent in criminal litigation. Do you have any thoughts on this process?

Peter Mahy: Well, I can see that DNA is very useful in a criminal case and it may solve a crime or prove that somebody is innocent. In the UK now, DNA is routinely used in family cases related to issues of paternity. In fact, DNA is used routinely in immigration cases. But it seems to me though that the essential issue to grapple with is when DNA should be taken without consent because that is an interference of people's rights, and so should it be taken on arrest or should it be taken when you are charged, or only voluntarily? And that is just the dividing line. I think there is a big mix up and a lot of false prophecy in the UK in how DNA should be used. The UK Government has always proclaimed the importance of DNA, but this question was also answered in the European case. Well that is not disputed. The question is, when you should take DNA from people who do not wish to give it?

Katina Michael: I have just finished reading Ron C. Michaelis, Robert G. Flanders and Paula H. Wulff, *A Litigator's Guide to DNA: from the Laboratory to the Courtroom* (2008) who state on p. 99 that the "ideal DNA database would contain the profiles of every person in the country" [United States]. But they go on to claim that "[a] database such as this will obviously never be compiled, so forensic analysts must use the data that have been collected, from a tiny portion of the population, to estimate the frequency of an allele in the larger population." Do you believe as Michaelis et al. do that the UK will never seek to implement a national DNA database? Is the idea as far-fetched as it might seemingly initially appear?

Peter Mahy: I think if we had not won the S & Marper case that this would have happened in the UK. There was mention in the UK courts that the Government was mostly relying on the principle that DNA was taken at the police station, that it was a historical fact and that it was not a big deal. And there were some reports that suggested that DNA samples should be taken from babies at hospitals when

they were born because at that point the procedure could be done fairly easily. And of course, you would not need to do it for everybody because of the capability to conduct familial searching with DNA. For instance, 15 to 20 million samples would probably be enough to identify almost anybody in the UK. It might not be that person but it might be their brother. And that clearly was attractive to the UK and I think that that might have come. But now because of the ECtHR judgment that is clearly in retreat now. I mean the Government here is proposing IDentification cards with biometric data on them. I think that is on very shaky ground now. My best guess now is that the Government is not going to go ahead with that, apart from the fact that they are fairly bankrupt. So initially yes, I think the idea was of a blanket coverage DNA database and that probably would have happened but I think now it is unlikely.

Katina Michael: Do you see the collection and storage of biometric data like fingerprints to be equally harmful as the collection and storage of DNA samples or profiles?

Peter Mahy: I do not see fingerprints as being as big an issue as DNA. I think with DNA it is the fear of future uses that worries people and people do not understand exactly what DNA is and what it could be used for. Whereas fingerprints are seen more as a signature and that less pieces could be extracted from it. But I think generally, especially with my clients, they are less concerned about fingerprints or a photograph than they are about DNA.

Katina Michael: I have a PhD student that is co-supervised by me and someone from the medical school that is working on the secondary uses of patient medical data including for instance the use of blood samples to aid in the discovery of cures. Her main aim is to develop a patient consent matrix. What I can say I am witnessing is a major push by the medical field, including medical practitioners and associated suppliers of medicines such as pharmaceutical companies to gain access to large amounts of what was once considered confidential databases in the hope that they can create medical breakthroughs. And there are also now quite a few health databases that contain hundreds of thousands of records and have been created voluntarily by the community adding their personal details to registers. Is it possible that we get to the point that the medical field almost overtakes the criminal/civil proceedings collection of DNA samples?

Peter Mahy: I was talking to some doctors in Leeds about this very topic earlier in the week. Doctors in hospitals are collecting blood samples every day for one thing or another. And I think there is a very important distinction they mentioned to me is that they have to ask the person if they consent at the start. And they also have the right to withdraw their consent and their details and samples taken off entirely in the future. And of course what we are talking about here is taking the DNA without consent and keeping them forever never bothering to take them off. But to me it seems that the big difference is consent.

Katina Michael: And how we would achieve true consent? Would you ask the

individual periodically whether they consent to their DNA data being stored on a medical database for medical discovery? Do you ask them every three months? This is a question we are finding hard to answer.

Peter Mahy: In the medical field of course, it may be, I do not know, say in three or four years time that they decide that DNA samples are going to be sold to insurance companies who are very interested in this data especially if you are going to be ill down the track. But at that stage a person might think, I do not want to be on that medical database anymore and I want to be taken off. I think those are the sort of scenarios that will cause the major development because then they could withdraw their consent. For instance, imagine a company who obtains this data and later turns out to be engaged in unethical practices, how would you then withdraw your consent. Again, to me, a major issue here is that you may give your DNA to a limited company who then sends it abroad. I do not really see how you can really control it and to ensure that if you withdraw consent at a later date; that you can indeed really get your DNA back or get it destroyed from the database?

Katina Michael: I am really interested in the role that self-interest groups have had in the S & Marper case from the very beginning to the present time. I have come up with the following groups, and I would like you to let me know if any are missing to your recollection. In no order of importance I have come up with the Nuffield Council on Bioethics, Liberty, GeneWatch, StateWatch, the Genetic Interest Group, and the NDNA Ethics Group, Amberhawk, and Where is Your Data.

Peter Mahy: There is a letter that was written by the interest groups to the Council of Ministers about a fortnight ago. And I think that all of these groups are important because they will influence particular decisions. You should add to your list Privacy International UK, Black Mental Health UK, Action on Rights for Children, and No2ID.

Katina Michael: One thing I am trying to do is to look at the S & Marper case from the view of different stakeholders- the government and policymakers, the citizens, the media, the academic papers that have been written on the S & Marper case such as case comments and notes, and of course, the self-interest groups that are lobbying on behalf of the rights of citizens.

Peter Mahy: To be perfectly honest what happened, is that while we were taking the case through the courts in the UK, we were on our own. In the Divisional Court there was little media interest, and nobody was interested. In the Court of Appeal, Liberty tried to intervene but they could not come to the hearing. In the House of Lords, again, Liberty intervened and they were threatened by the Government that if they did and they came to the hearing there would be costs against them and Liberty was fearful of that. So in fact, Liberty did not come to the House of Lords. So we were really the only ones against the Police and the Government and we were hugely outgunned. It was not until we got to the European Court that Liberty put some submissions in, and importantly Privacy International UK put in some really good work but for the actual ECtHR hearing we were on our own again.

There was seriously little back up then, but now that the judgment has come to pass there is a lot of interest from interest groups who are doing good work. Non-government organizations have a right to participate in the Council of Ministers debate, and that is why now they actually have some power.

Katina Michael: Peter, could you tell me how to describe your exact role on the S & Marper case?

Peter Mahy: The solicitor, who acted for the claimant in the S & Marper v United Kingdom case.

Katina Michael: And can I ask, why Mr S and Mr Marper? How did it come to pass that you chose these two individuals? Had they approached Howells LLP?

Peter Mahy: So the reality was that South Yorkshire Police had written a letter to all solicitors saying that because the law had changed they were going to keep all DNA samples of people. In other words they were saying- "[s]top asking for the DNA samples to be destroyed." And then when the email came around and I read this letter, I immediately thought, well that does not really sound right and we should challenge it. And very quickly I had Mr S and Mr Marper in the office who had written to the police asking for destruction of their DNA samples. I think till that point, I do not really think anyone else had really thought about it as the legislation in the UK was just out, and few perhaps saw it as an issue and worth challenging.

Katina Michael: Just as a final summary Peter, what were the tangible/intangible or explicit/implicit impact(s) of the ECtHR ruling on the United Kingdom?

Peter Mahy: Tangible is that the ECtHR ruling has created change and at the moment there is a lot of debate, a lot of talking between parties here. I think in a way it has drawn a line in the sand, and hopefully in the next 10-20 years we will look back and say that was an important case. That that was a case, where we took a good look at what was going on in the UK and put a stop to the erosion of rights.

Katina Michael: Any final comments that you might have on this S & Marper case?

Peter Mahy: I think one thing that is important to mention is how poorly funded we were. We were granted some legal aid from the European Court which was 2,613 euros. That was for myself and the barrister and included traveling expenses. So we were probably looking at something like 600-1,000 euro for the both of us, some 200-300 pounds each. It was an immense amount of work- boxes and boxes of documents. But at the same time, the Government lawyers were probably getting paid about 200-300 pounds per hour for the case. And we expect that the UK Government spent hundreds of thousands of pounds, if not millions of pounds just on the hearing. We made a request to freedom of information from the UK Government and they refused them, on the basis that this information was commercially sensitive. I think this just highlights the inequality of people trying to win a case versus the Government and the State. And now that we won the case we got paid fairly reasonably but we are sure, nothing like what the Government got paid. I think it shows the importance of people taking a stand but it is very difficult to communicate that lesson.

Katina Michael: Well, I for one, having researched this case over the last 12 months, am quite in awe of what you have achieved. And I am unsure if you perceive the great importance of S & Marper for other nation states, but this case ruling will set a precedent for others to follow. Thank you for conducting this interview with me.

15

Intelligence, Ethics and the Creation of Certainty from Uncertainty

Jeff Corkill
Edith Cowan University

Abstract

Intelligence is acknowledged as a key function of modern law enforcement demonstrated in the common use of the term 'intelligence led policing' in various parts of the world. Furthermore it may be argued that the emergence of intelligence led policing is a response to the avalanche of information inundating police. Intelligence by its very nature has been a secret business, arcane and steeped in mystery, a profession long hidden away and rarely credited for policy or operational success yet often blamed when poor policy or operational decisions result in public humiliation. The Haneef case has been argued by some an abuse of intelligence on the part of the AFP argued by others a failure of intelligence. It may be argued also there is a perception on the part of some in the community that intelligence is a weapon of politics used for the purpose of justifying unpopular political decisions rather than being professional objective insight to aid decision making. This politicisation of intelligence gives rise to a debate on the ethics of intelligence in terms of collection, analysis and the subsequent application of intelligence products. Intelligence analysts process complex problems including moral and ethical issues, which may question values, beliefs and assumptions; the outcomes of which may impact on the individual through to national security levels. This study will build on the limited law enforcement knowledge base and extend it into an examination of ethical analytical judgement and decision-making by analysts within a law enforcement environment.

Keywords: intelligence, ethics, uncertainty, law enforcement, politics

16

Counter Terrorism and Access to Justice: Public Policy Divided?

Mark Rix

University of Wollongong

Abstract

This paper will consider Australia's counter-terrorism strategy and highlight the implications of its strategy for its citizens' and residents' access to justice. Access to justice, encompassing the ability of individuals, including persons suspected of terrorism offences *and* non-suspects, effectively to exercise their human and legal rights, can be an important curb on state power. But, in another equally important sense, providing individuals with access to justice also protects national security by helping to ensure that the law enforcement and security agencies focus their efforts on genuine terror suspects rather than wasting their resources on investigating and attempting to prosecute genuine non-suspects. Accordingly, access to justice in the context of counter-terrorism, and more broadly, involves such things as suspects' (and, non-suspects') *enforceable* rights: to be represented by competent, independent and affordable legal counsel (thus including the availability of adequate legal aid); to the presumption of innocence; to a fair trial; not to be convicted of a terrorism offence through the use by police, intelligence and prosecuting authorities of evidence that would be inadmissible in 'normal' criminal proceedings; not to be subject to indefinite detention (particularly so-called pre-charge detention); and, so on. Using the access to justice benchmark, the paper will investigate and assess the conditions imposed on legally-aided clients in Australian terrorism cases in the selection of their legal representatives. It will also briefly compare these conditions with similar measures for protecting national security information in criminal proceedings adopted by 'leading' Western states like the United States, Canada and Great Britain.[1]

Keywords: counter-terrorism, justice, public policy

1 My deep gratitude to Jen Hawksley for her fantastic research assistance in the preparation of this paper.

1 Introduction

Legal aid is an important mechanism for ensuring that individuals who cannot afford to engage a private legal practitioner to represent them are put on a roughly equal footing to those who are able to afford private legal representation and therefore to obtain an equivalent measure of access to justice (see Rix 2008a for an analysis of the Australian legal aid system, and the associated community legal sector). By providing poor, disadvantaged and excluded Australians with the opportunity to pursue just outcomes of the civil, administrative, family and criminal law matters they seek to have resolved, legal aid (and the community legal sector with which it is closely associated) makes a significant contribution to enhancing the cohesiveness and inclusiveness of Australian society. This is a fundamentally important role for, after all, access to justice and equality before the law underpin the legitimacy of the legal system and the willingness of individuals to accept and comply with the law. In this way, legal aid helps to uphold the rule of law and prevent the social discord and fragmentation that would result from disaffected individuals and groups choosing for lack of available alternatives to take the law into their own hands.

This paper is especially concerned with the role of legal aid in providing access to justice to individuals involved in criminal law matters, in particular, terrorism cases. Since the commencement of the global 'war on terror' in 2001, this has become a difficult and complex area of public policy and the administration of justice for liberal democracies such as Australia. The state, through the elected government, has a duty to respect and protect human rights and uphold the rule of law. But it also has an equally weighty duty to protect and safeguard the country's national security from such threats as terrorist violence and attacks. The legitimacy of the state, and government, in liberal democracies is largely derived from its ability at once to protect the human rights of its citizens, especially through upholding the rule of law, and to safeguard the nation's security as the basic precondition of the country's social, economic and political life being able to continue with minimal disruption. Genuine threats to national security such as those mounted by determined terrorist groups and individuals can equally be threats to the rule of law and to human rights. But the government's efforts to safeguard the country's national security, and by extension (if not open acknowledgement) the rule of law and human rights, can correspondingly and paradoxically undermine the rule of law and the human rights of its citizens. The paradox is explored in this paper through an investigation of the conditions imposed on legally-aided clients in terrorism cases in the selection of their legal representatives and the implications of imposing these conditions, on the one hand, for the rule of law and human rights and, on the other, for Australia's national security. Some tentative suggestions as to how the paradox could be resolved are also offered beginning with a repudiation of the false zero sum 'equation' widely thought to represent or simulate the relationship between national security and the rule of law and human rights (that is, more of one necessarily means less of the others and vice versa).

2 Counter-terrorism and Fair Trial Requirements

Writing in *The Sydney Morning Herald* on February 24 this year, George Williams who is the Anthony Mason Professor of Law at the University of New South Wales pointed out that 'From September 11 [2001] to the end of the Howard Government, Parliament passed 44 anti-terrorism laws, an average of one every seven weeks' which is an unenviable legislative record with 'no parallel in any other democratic nation (Williams 2009).' These many laws include provisions allowing for the detention in secret of non-suspects merely for intelligence-gathering purposes, reversal of the onus of proof (cancelling the presumption of innocence), removal of the right to silence and limitations on access to legal representation (see Rix 2006 and Rix 2008). It is the restriction on a legally-aided client's right to be represented by a lawyer of their own choosing contained in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (hereafter referred to as the NSI Act) which is the focus of this paper. The inclusion of this apparently minor and inconsequential provision in the NSI Act has serious implications for national security and for human rights and the rule of law. Before examining in greater depth the provision and its implications, however, the paper first considers how imposing conditions on a person's ability to choose their own legal counsel affects their right to receive a fair trial.

George Williams' piece in *The Sydney Morning Herald* appeared just after the release of the International Commission of Jurists' (ICJ) report dealing with terrorism, counter-terrorism and human rights. The release of this report is significant because, as Williams observes, the ICJ is '[o]ne of the world's most respected legal bodies' (Williams 2009), is a non-governmental organisation which steadfastly adopts a non-partisan approach in all of its work and which focuses on upholding international law and the rule of law in order to advance human rights throughout the world. Titled *Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights*, the report provides a comprehensive international survey of the effect which the counter-terrorism measures adopted by more than 40 national governments since 2001 has had on human rights and the rule of law in their countries. It should be noted here that the Eminent Jurists Panel comprises 'eight distinguished jurists from all regions of the world, is an independent body, [and is] supported by ICJ Secretariat staff (ICJ 2009: v).'

Restricting access to legal representation in criminal proceedings has the potential to undermine one of the cornerstones of the criminal justice system that has come to characterise liberal democratic states. This is the right to a fair trial 'before an independent and impartial judiciary', a principle regarded as being so fundamental to international human rights law (see, for example, Article 14 of the *International Covenant on Civil and Political Rights* (ICCPR)) that the UN Human Rights Committee has stated that it 'cannot be departed from, even at a time of

emergency (ICJ 2009: 143).'[2] Similarly for international humanitarian law, fair trial requirements even during armed conflicts are 'enshrined in Common Article 3 of the *Geneva Conventions*, and in the relevant provisions of the *Geneva Conventions* (ICJ 2009: 143).'[3] Having prompt access to legal counsel of an individual's own choice is just one of the requirements of a fair trial and complements the other requirements that are stipulated in international humanitarian law and international human rights instruments like the ICCPR. The other requirements, more correctly 'minimum guarantees', contained in the ICCPR (Article 14) include that a person be informed promptly and in full of the charge against her/him, that a person facing a criminal charge be presumed innocent until found guilty according to law (beyond reasonable doubt), that the person be given adequate time and resources to prepare her/his defence including having access to legal counsel of her/his own choosing and that the person be present at their trial and be able to defend her/himself in person or with the assistance of legal counsel of her/his own choosing (ICJ 2009: 143, n. 386). The right to a fair trial is fundamental to international human rights law and international humanitarian law and this right encompasses the minimum guarantee that a person is able to be represented by legal counsel that she/he freely chooses. Thus, any restraint or limitation on the ability of a person to choose their own legal counsel in criminal proceedings imposes an unwarranted condition on their right to a fair trial, a right that is so fundamental that it cannot be departed from even in situations of armed conflict. The so-called 'war on terror' is not an armed conflict as such and imposing conditions on a person's right to choose counsel in terrorism cases, therefore is a serious infringement on their right to a fair trial which is not even able to fall back on the pseudo-justification that it is an exceptional measure required to deal with exceptional circumstances.[4]

The following section begins with a brief history and overview of the NSI Act. It then investigates the provisions contained in the Act which limit the information (that is, information that is regarded as having relevance to national security as broadly defined) that can be withheld from the defendant and/or their legal representative. This is followed by an examination of the restriction the NSI Act imposes on a

2 It is seems incongruous, then, that as the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Martin Scheinin) blandly noted in his August 2008 Report to the UN General Assembly, 'In situations where counsel is assigned under legal aid, however, the Human Rights Committee has accepted that limitations may be imposed on the right to choice of counsel (UN 2008: 19).' The Special Rapporteur cites in a footnote (n. 91) Teesdale v. Trinidad and Tobago, Human Rights Committee Communication No. 677/1996, CCPR/C/74/D/677/1996 2002), para. 9.6.

3 The Additional Protocols I and II to the Geneva Convention dealing with the protection of civilians during respectively international and non-international armed conflicts both affirm fair trial requirements.

4 The inappropriateness of the phrase 'war on terror' and associated 'war paradigm' is dealt with at length in *Assessing Damage, Urging Action*, Chapter Three: The legality and consequences of a 'war on terror' (ICJ 2009: 49-66).

legally-aided client in a terrorism case to have access to legal counsel of their own choosing.

3 The NSI Act

The *National Security Information (Criminal Proceedings) Act 2004* passed into law on 8 December 2004, with its key provisions commencing on 11 January the following year. The latter was the date on which the *National Security Information (Criminal and Civil Proceedings) Regulations 2005* (the NSI Regulations) also commenced. The NSI Regulations prescribe how national security information should be stored, handled and destroyed. The Requirements for the Protection of National Security Information in Federal Criminal Proceedings and Civil Proceedings (the NSI Requirements), which are incorporated in the Regulations, include more detailed specifications for how national security information should be accessed, stored and handled and also deal with a number of relevant physical security considerations. The NSI Act 2004, which dealt only with criminal proceedings, was amended by the *National Security Information Legislation Amendment Act 2005* to extend the protection from disclosure of "security sensitive information" by including "certain civil court proceedings" (Australian Laws to Combat Terrorism' n.d.). *The National Security Information (Criminal and Civil Proceedings) Act 2004*, commencing 3 August 2005, is the result. Thus, through amendment, the NSI Act was brought into line with the Regulations (and, Requirements) which it is supposed to underpin.

According to the Federal Attorney-General's Department, the NSI Act, NSI Regulations and NSI Requirements provide

> a comprehensive regulatory framework for the disclosure, storage and handling of all NSI involved in federal criminal proceedings or civil proceedings, whether in documentary or oral form. The NSI Act applies from the pre-hearing stages through to completion of appellate proceedings, thereby enabling the parties to identify and bring forward any NSI issues as early as practicable (AGD 2008: 6).

The object of the Act, as should already be apparent, is to prevent the disclosure of information in federal criminal proceedings or civil proceedings that could prejudice national security unless non-disclosure would severely impede the administration of justice. The NSI Act, Regulations and Requirements are all based on a broad view of what 'national security' means. In the Act (Section 8), 'national security' is defined to encompass '"Australia's defence, security, international relations or law enforcement interests"' the latter included 'to ensure that law enforcement information which is connected to national security, including intelligence collection methods and technologies, is not excluded from protection' under the Act (AGD

2008: 10).[5] While the NSI Act does not contain a single definition of 'national security information' it does classify information into two different categories: 1. information simply relating to national security and which itself, or its disclosure, could *affect* national security. 2. Information which could *prejudice* national security if disclosed. Section 24 of the NSI Act requires the Attorney-General to be notified if the information or its disclosure would affect national security. Where the Attorney-General comes to the view that disclosure of the information would prejudice national security, he or she may issue a certificate which limits disclosure (section 26). But what is 'information'? As far as the Act is concerned (section 7) '"information" means information of any kind, whether true or false, whether in material form or not and whether it is in the public domain or not' including 'an opinion or a report of a conversation (AGD 2008: 11).' Thus, as far as the NSI Act is concerned 'information' can mean almost anything and is therefore a nearly meaningless term. Nevertheless, attaching such a broad and all-encompassing meaning to 'information' coupled with the inclusion of 'law enforcement interests' in the definition of national security gives the Executive enormous scope for unwarranted interference in the administration of justice. This is a matter which is taken up in the final section of the paper.

The Attorney-General can issue several types of certificates in situations where she/he considers either that information will be disclosed that is likely to prejudice national security or that a witness will disclose information that is likely to prejudice national security. A criminal non-disclosure certificate can be issued when the Attorney-General has been informed under section 24 or subsection 25(6) that a disclosure of information is expected or that information will be disclosed by a party to the proceeding or a witness and she/he believes that the information to be disclosed is likely to be prejudicial to national security. The Attorney-General can issue a criminal witness exclusion certificate when she/he has been notified under section 24, or expects for any reason 'that a person whom the prosecutor or defendant intends to call as a witness may disclose information by his or her mere presence' and believes that the disclosed information is likely to be prejudicial to national security (AGD 2008: 17 and 18). The NSI act also enables the Attorney-General to issue civil non-disclosure (subsection 38F(2)) or civil witness exclusion (section 38H) certificates under arrangements that are 'substantially similar' to those in criminal proceedings. An exception is where the Attorney-General is a party to the civil proceeding in which case 'any references to the Attorney-General means the alternative Minister appointed to perform functions under the NSI Act (AGD

5 It is noted in *Assessing Damage, Urging Action* that '[t]hese provisions [had been] criticised on the grounds that the scope of information that could be withheld was excessively broad (ICJ 2009: n. 428, p. 152). Concerns regarding both the scope of 'information' and the broad definition of 'national security' were also expressed in many submissions to the Senate Legal and Constitutional Legislation Committee's (SLCLC) inquiry in the provisions of the National Security Legislation Amendment Bill 2005. See SLCLC (2005) Provisions of the National Security Information Legislation Amendment Bill 2005, especially pp. 33-36.

2008: 31).'

When a criminal non-disclosure or witness exclusion certificate is provided to the court it must hold a closed hearing in order to make a determination on whether to make an order under section 31 regarding 'whether it will maintain, modify or remove the restriction on the disclosure of information or the calling of witnesses (AGD 2008: 19).' A closed hearing precedes the substantive hearing if a certificate is received before the substantive proceeding begins and is held on adjournment of the substantive proceeding when it is received after the proceeding has begun. A closed hearing (section 29) deals strictly with the two matters of whether to allow a witness to be called and whether to allow disclosure of information that is likely to prejudice national security and, if so, what form it should take. In sum, '[t]he closed hearing is solely concerned with contested issues of disclosure preliminary to, but outside of, matters to be adjudicated (including the relevance and admissibility of NSI) in the substantive hearing (AGD 2008: 20).' Defence counsel and court staff who do not have security clearances can be excluded from a closed hearing when disclosing information to them is believed to have the potential to prejudice national security. The persons who can be present at a closed hearing are the magistrate, judge or judges hearing the case, the prosecutor, and the Attorney-General or her/his legal representative if she/he exercises her/his right to intervene (section 30). Court officials, the defendant, the defendant's legal representative and witnesses can only be present subject to the court's discretion.

In *Assessing Damage, Urging Action*, the Eminent Jurists Panel noted that in Australia, as in Canada, a defendant may appeal against the issuing of a criminal non-disclosure or witness exclusion certificate. However, the Panel was concerned that, in Australia, 'the court is required to give greatest weight to the question of "the risk of prejudice to national security" rather than to the needs of the accused (ICJ 2009: 153).' Requiring courts to make 'national security' a higher priority than the needs and rights of the accused (and, even *non*-suspects) is consistent with other aspects of the NSI Act, and of Australia's counter-terrorism legislation more generally (see, for example, Rix 2008).

4 Legal Counsel of One's Own Choosing?

The Commonwealth Legal Aid Application Guideline 7 deals with 'National security matters—requirement for security clearance'. Guideline 7 commenced operation on 4 July 2006 and replaced the former Criminal law Guideline 9 'National Security matters'. The exceptions in the discarded Guideline 9, which under certain circumstances enabled assistance to be provided even when a legal aid client's legal representative did not hold a security clearance, were omitted from Guideline 7. Guideline 7 was introduced to ensure compliance with the NSI Act particularly as it relates to disclosure of NSI in Commonwealth criminal and civil (including family) matters. According to the Attorney-General Department's Practitioners' Guide to the NSI Act, '[t]he Commonwealth Legal Aid Amendment Guidelines do

not restrict a legally-assisted client's ability to *nominate* a preferred legal practitioner (AGD 2008: 28; emphasis added.)' Nominating a preferred legal practitioner is one thing, actually being able to choose a legal practitioner is quite another. Before or during a federal criminal proceeding, the Secretary of the Attorney-General's Department may provide written notice to the defendant's legal representative or associate assisting the representative to the effect that information may be disclosed in the proceeding which has the potential to prejudice national security (section 39). In such cases, the defendant's legal representative and her/his assistants can apply to the Attorney-General's Department for a security clearance, a process which 'is conducted at arm's length from the agencies involved in prosecutions (AGD 2008: 29).' After a section 39 notice has been issued, the legal representative of a legally-aided client will only receive further payments under the legal aid scheme subject to being issued with a security clearance or having applied for a security clearance (payments under a grant of legal aid may be made for work completed before the section 39 notice was issued). A legal representative is required to apply for a security clearance within 14 days of receiving a section 39 notice. This is precisely where the freedom to nominate a preferred legal practitioner becomes a highly conditional choice of legal representative. When the legal representative fails to apply for a security clearance, '[t]he court may then advise the defendant of the consequences of being represented by an uncleared legal representative [that is, the possibility that the legal representative will not have access to NSI which is relevant to the proceedings] and may recommend that the defendant engage a legal representative who has been given, or is prepared to seek, a security clearance (AGD: 2008 30).' The level of security clearance required by legal representatives, court personnel, and so on is calibrated to the highest level of NSI classification involved in a case so that, for example, should 'Secret' be the highest level of NSI classification a 'Secret' level security clearance is required.

The NSI provisions pertaining to civil cases 'mirror' those applying in criminal cases. However, there is an important, extra provision (subsection 39A(6) of the NSI Act):

> In recognition of the additional financial burden involved in engaging a security-cleared legal representative to attend a closed hearing, a self-represented litigant involved in a civil matter who is refused a security clearance at the appropriate level would be eligible to apply for financial assistance under the Special Circumstances Scheme. If approved, this would provide financial assistance for the legal costs associated with engaging a security-cleared legal representative to attend the closed hearing and any related appeal. The opportunity for such unrepresented parties to access financial assistance in order to retain a security-cleared lawyer is an important component of the scheme (AGD 2008: 42).

This extra provision is an acknowledgement of the additional financial burden to a self-represented litigant in a civil proceeding should they wish to have a legal

representative attend a closed hearing. However, consistent with the provisions relating to criminal proceedings, the choice of legal representative is constrained by the need for the nominated representative to have a security clearance at the appropriate level.

5 Models and Precedents

According to the Practitioners' Guide, the provisions for closed hearings contained in the NSI Act are not as broad 'in ambit' as the statutory procedures for protecting NSI in court proceedings that operate in the UK, Canada and the US. In these other jurisdictions, prescriptions for the closure of proceedings cover the substantive hearing as well as the 'more confined "voir dire" segment' of a trial. However, the Guide also points out that '[i]n developing its [Australia's] legislative regime for the protection of NSI in court proceedings, careful consideration was given to the statutory approaches taken in the United States, Canada and the United Kingdom (AGD 2008: 7).' In the United States, as with Canada, statutory NSI protection procedures have been in operation for more than 20 years. The relevant acts are the US Classified Information Procedures Act 1980 (the US CIPA) and the Canada Evidence Act 1985. Both of these Acts place an obligation on a criminal defendant who expects to call NSI as evidence to notify the Government of this eventuality and 'also require that the nature and admissibility of such evidence be determined in closed hearings (AGD 2008: 7).' In the USA, in the event that a court determines the admissibility of NSI the US Government can seek orders under the CIPA enabling a redacted version, a summary of the relevant facts or 'an admission of relevant facts' to be substituted for the original information and to be called as evidence.[6] As for Canada, the Attorney-General first decides whether the NSI can be disclosed, a decision which can be challenged before a court. If it is determined by the court that the NSI is admissible it can then authorise a summary or a 'written admission of facts' to be substituted for the NSI. However, where a court does not permit a

6 But see the 2008 article in the *Harvard Law Review* on withholding classified information to protect sensitive information in criminal proceedings (cited here as Harvard Law Review 2008). This article, written in response to the decision of the Second Circuit court to affirm a decision of the District Court for the Northern District of New York to withhold certain 'classified information that might otherwise have been discoverable', under the provisions of the CIPA Act. The article notes that the court cited a 'highly controversial' privilege in civil litigation that 'demands great deference to the executive branch's desire to protect sensitive information (p. 819).' The case involved the arrest and charging with numerous offences of Yassin Aref and Mohammed Hossain in connection with a police operation centring on the sale of a surface-to-air missile. In writing for the 'unanimous panel', Judge McLaughlin of the Second Circuit began by noting that "although CIPA does not itself *create* a privilege", it "*presupposes* a government privilege against disclosing classified information" (p. 820). As the *Harvard Law Review* article points out in relation to this privilege, '[t]he political controversy and precedential implications that the state secrets doctrine has developed in civil litigation could undermine the legitimacy of prosecutions involving classified information, while spreading the privilege's use to criminal law may weaken the political checks necessary to restrain its use in civil litigation (p. 819).'

summary or admission of relevant facts to replace the NSI 'the Attorney-General may issue a certificate prohibiting disclosure of the information (AGD 2008: 8).'[7] In the UK, there is no single equivalent of the US CIPA or Canada Evidence Act. Instead, two acts deal with how NSI should be used in criminal proceedings: the Criminal Procedures and Investigation Act 1996 codifies the public interest immunity principle and the Official Secrets Act 1920 sets out other procedures for protecting NSI.[8] The restrictions on court reporting contained in the Criminal Procedures and Investigation Act section 37 have been incorporated into subsections 29(5) (criminal proceedings) and 38I(5) (civil proceedings) of the NSI Act (AGD 2008: 8).

According to the Practitioners' Guide, and without citing any substantiating evidence, the security clearance procedure under the US CIPA '…has been accepted by the US legal profession as being part of its obligations to properly represent clients (AGD 2008: 27).' The Guide also asserts that undertaking security clearances of legal representatives has been validated by 'recent US case law' as the 'best mechanism to prevent unauthorised disclosure of classified information in the custody of the court (AGD 2008: 27).'[9] As for Canada, 'security cleared counsel appear before hearings conducted by the Security Intelligence Review Committee and are appointed from a panel of security cleared lawyers (AGD 2008: 27-28).' The UK Juries Act authorises 'limited' security assessments of potential jurors conducted consistent with guidelines issued by the Attorney-General.

6 The Zero Sum Equation: Does Weakening the Rule of Law and Lessening Human Rights Protections in Fact Increase National Security?

The requirement that legal counsel representing a legally-aided client in a terrorism case obtain a security clearance makes the administration of justice unwieldy and inefficient and leaves it highly susceptible to unwarranted executive

7 For the difficulties encountered in 'balancing' the protection of national security and the safeguarding of human rights in the Canadian context see, for example, Adelman 2006 and Theroux and Karpinski 2008. Both these papers discuss the provisions of the Canada Evidence Act with regard to the nature and admissibility of NSI as evidence and the security clearance process for legal counsel in terrorism cases (amongst others).

8 Duncan Campbell, in a 2008 piece in *The Guardian*, points out that 't]he [UK] government's use of the Official Secrets Act to prevent issues of public interest being published is also [along with libel laws and other controls introduced in recent counter-terrorism legislation] condemned in an intervention from the UN [committee on human rights] which warns that public servants are being gagged even where national security is not at risk (Campbell 2008).' See also Ian Cram (2009) *Terror and the War on Dissent: Freedom of Expression in the Age of Al-Qaeda*, Springer, Berlin which examines freedom of expression in the context of national security and counter terrorism in the UK, particularly the provisions and use of the Official Secrets Act to prevent disclosure of sensitive information.

9 The Guide cites US v Usama Bin Laden 58F Supp 2d 113 (S D NY 1999) as a case in point (n. 78, p. 27).

interference. It holds legally aided people hostage to the discretion of the Secretary of the Attorney-Generals' Department regarding the issuing of national security notifications and to the Department for determination of the appropriate level of clearance required by a legal representative. The process of issuing a national security notification and determining whether a security clearance is required and, if so, at what level, appears to be a completely arbitrary one, lacks transparency and is not open to public scrutiny.[10] Thus legal practitioners and civil society organisations which seek to hold executive government and its agencies accountable and answerable for their actions have no effective means of keeping this process under scrutiny and review. Just as importantly, this requirement provides the executive arm of Government with wide access to information about individual lawyers and therefore opens up the possibility of misuse and abuse of the information, and the access to it, by the executive and the national security authorities which act on the executive's authority.

In imposing restrictions on the ability of a legally-aided person to choose their own counsel, the NSI Act 'detracts significantly from the guarantee in article 14(3) of the ICCPR that all persons have access to a legal representative of their own choosing, and that such representation be provided by the State in cases where the person does not have sufficient means to pay for it' themselves (Law Council of Australia 2008: 81). This is a serious threat to the right to a fair trial.

> In the view of the Law Council [of Australia], the security clearance system for the legal profession under the Act threatens the right to a fair trial in two ways. First, it restricts a person's right to a legal representative of his or her choosing by limiting the pool of lawyers who are permitted act in cases involving classified or security sensitive information. Secondly, it threatens the independence of the legal profession by allowing the executive arm of government to effectively "vet" and limit the class of lawyers who are able to act in matters which involve, or which might involve, classified or security sensitive information. By undermining the independence of the legal profession in this way, the right to an impartial and independent trial with legal representation of one's own choosing is similarly undermined (Law Council of Australia 2008: 80).

By providing the executive arm of Government with greater powers at the expense both of the human rights of individuals involved in terrorism cases and of the independence of the legal profession, the NSI Act opens the door to the arbitrary exercise or abuse of state power. It also dangerously weakens rather than enhances Australia's national security.

10 Similar concerns were raised in a number of submissions to the SLCLC's inquiry into the NSI Amendment Bill (see SLCLC 2005, especially pp. 26-27). See also comments made by then Chief Justice of the Supreme Court of Tasmania Peter Underwood and then Chair of the Criminal Bar Association of Victoria Lex Lasry (Underwood 2006 and Lasry 2004).

In the Additional Comments and Points of Dissent attached to the SLCLC Report on the NSI Amendment Act, Senator Brian Greig of the now Federally-defunct Australian Democrats made a number of important points. The Democrats were concerned that the Act would undermine Australia's national security, rather than enhance it. '[I]n the minds of many Australians', the Democrats suggested, 'national security means the protection of the physical safety *and* fundamental rights of all Australians (SLCLC 2005: 50; emphasis added).' In putting forward this suggestion, the Democrats in a subtle way advanced a notion of national security that includes both physical safety and fundamental rights and which is therefore at variance with the conventional view. According to the conventional view, there are circumstances in which safeguarding national security requires the protection of human rights and the rule of law to be a secondary consideration for the Government. Those who hold to the conventional view regard the 'war on terror' as just such a circumstance requiring the Government to adopt exceptional measures to deal effectively with the exceptional threat to physical safety and fundamental rights that is believed to be presented by groups and individuals who are intent on perpetrating terrorist violence. The conventional view is underpinned by the zero sum equation which implicitly (and, sometimes even explicitly) equates, on the one hand, the protection of human rights and the rule of law with reduced national security and, on the other, increased national security with fewer and weaker human rights protections and a weakening of the rule of law.[11] The new notion advanced by the Australian Democrats escapes the zero sum equation by rejecting the presumption that human rights (and the rule of law) and national security are necessarily in opposition to or inconsistent with each other. Instead, the protection of human rights and the rule of law is regarded as being a fundamental aspect of national security and *its* protection. Such a notion of national security escapes the flaw in the conventional view, namely, the privileging of state security over the security and liberty of the person and its inherent risk of state power being misused or abused.

7 Conclusion

The NSI Act imposes serious restrictions on the ability of a legally-aided individual in terrorism cases to be represented by a legal practitioner of their own choosing, threatening the right of such an individual to a fair trial. The right to legal counsel of one's choice is one of the fair trial requirements, or minimum guarantees, recognised in both international human rights law and international humanitarian law. The zero sum equation that underpins the conventional view of national security is based on the two-part assumption that enhancing national security reduces human rights protections and weakens the rule of law and that strengthening human rights and the rule of law weakens national security. On this flawed logic, then,

11 Dangerous thinking of this sort is evident in the Attorney-General Robert McClelland's praise of Singapore's approach to national security and counter-terrorism (see Dorling 2009). See also Mr McClelland's address to the 7th Annual National Security Australia Conference (McClelland 2009).

even though the NSI Act threatens the right to a fair trial it nevertheless enhances Australia's national security. However, the NSI Act is a dangerous piece of legislation that, far from enhancing national security, seriously erodes it. A new conception of national security is urgently required which regards protecting human rights and upholding the rule of law as being fundamental to the safeguarding of Australia's national security. With this conception of national security, the NSI Act and much of the other legislation included in Australia's counter-terrorism regime could be discarded (and, hopefully forgotten altogether).

References

Adelman, H 2006 'Canada's Balancing Act: protecting human rights and countering terrorist threats'. Paper presented at the annual meeting of the International Studies Association, San Diego, California, 22 March. Available at: http://www.allacademic.com/meta/p99019_index.html (accessed 24 September 2009)

Attorney-General's Department (AGD) 2008 National Security Information (Criminal and Civil Proceedings) Act 2004: Practitioners' Guide (June). Available at: http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(3A6790B96C927794AF1031D9395C5C20)~Practitioners++Guide+to+NSI+Act+-+FINAL1.pdf/$file/Practitioners++Guide+to+NSI+Act+-+FINAL1.pdf. (accessed 12 March 2009).

Australian Government n.d. Australian Laws to Combat Terrorism: National Security Information (Criminal and Civil Proceedings) Act 2004. Available at: http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/D16EA21E0D42285CCA256FCC0015F336?OpenDocument (accessed 12 March 2009)

Campbell, D 2008 'Labour warned over limits to free expression', *The Guardian*, 15 August. Available at: http://www.guardian.co.uk/ (accessed 23 September 2009)

Dorling, P 2009 'Attorney-General praises Singapore terrorism policy', *The Canberra Times*, 19 March. Available at: http://www.canberratimes.com.au/news/world/world/general/attorneygeneral-praises-singapore-terrorism-policy/1463395.aspx (accessed 20 March 2009).

Harvard Law Review (2008) 'Criminal Law – Classified Information Procedures Act: Second Circuit holds that Government may withhold classified information unless information would be "relevant and helpful" to defense – United States v Aref, 533 F3d 72 (2d Cir.2008)', *Harvard Law Review*, Vol 122, pp.819-826. Available at: http://www.harvardlawreview.org/issues/122/dec08/recentcases/us_v_aref.pdf (accessed 22 September 2009)

International Commission of Jurists (ICJ) 2009 *Assessing Damage, Urging Action*. Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights. Available at: http://ejp.icj.org/IMG/EJP-Report.pdf (accessed 17 February 2009)

Lasry, L 2004 Correspondence dated 2 July 2004 from Lex Lasry QC, Chairman of the Criminal Bar Association of Victoria to Philip Bailey, Acting Secretary, Legal & Constitutional Committee, Australian Senate. Available at: http://www.crimbarvic.org.au (accessed 24 September 2009)

Law Council of Australia (LCA) 2008 Anti-Terrorism Reform Project: A consolidation of the Law Council of Australia's advocacy in relation to Australia's anti-terrorism measures. Available at: http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=DB5ED540-1E4F-17FA-D27B-557BADC6D4F7&siteName=lca (accessed 20 March 2009).

McClelland, R 2009 Speech at the 7th Annual National Security Australia Conference, Darling Harbour, Sydney, 23 March. Available at: http://www.attorneygeneral.gov.au/www/ministers/RobertMc.nsf/Page/Speeches_2009_23March2009-7thAnnualnationalSecurityAustraliaConference (accessed 23 March 2009).

Rix, M 2006 'Australia's Anti-Terrorism Legislation: The National Security State and the Community Legal Sector', *Prometheus*, vol. 24, no. 4 (December), pp. 429-439.

Rix, M 2008 'Australia and the "War against Terrorism": Terrorism, National Security and Human Rights', *Crimes and Misdemeanours*, 2/1, pp. 40-59

Rix, M 2008a 'Legal Aid, the Community Legal Sector and Access to Justice: What has been the Record of the Australian Government?' in Asha B. Joshi (ed.), *Legal Profession: Modern Approach*, The Icfai University Press, Hyderabad India, pp. 85-111

Senate Legal and Constitutional Legislation Committee 2005 Provisions of the National Security Information Legislation Amendment Bill 2005. Available at: http://wopared.parl.net/senate/committee/legcon_ctte/completed_inquiries/2004-07/national_sec/report/report.pdf (accessed 17 March 2009).

Theroux, C and Karpinski, M 2008 'The dilemmas of ensuring national security while protecting human rights: perspective from the Canadian Human Rights Commission'. Paper presented at the annual meeting of The Law and Society Association, Montreal, Quebec, 27 May. Available at: http://www.allacademic.com/meta/p235806_index.html (accessed 24 September 2009).

UN 2008 Report to the General Assembly of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 6 August. Available at: http://daccessdds.un.org/doc/UNDOC/GEN/N08/451/82/PDF/N0845182.pdf?OpenElement (accessed 16 March 2009).

Underwood, P 2006 Speech by the Honourable Chief Justice Peter Underwood AO to the Law Society of Tasmania Dinner. 13 May. Available at: http://www.supremecourt.tas.gov.au/publications/speeches/underwood/lawsoc0506 (accessed 24 September 2009).

Williams, G 2009 'Time to Change Terrorism Laws', *The Sydney Morning Herald*, 24 February. Available at: http://www.smh.com.au/opinion/time-to-change-terrorism-laws-20090223-8fr1.html?page=-1 (accessed 24 February 2009).

Author Biographies

Ms Roba Abbas graduated with first class honours in Information and Communication Technology (majoring in Business Information Systems) from the University of Wollongong Australia, in 2006. She is currently a PhD candidate in the School of Information Systems and Technology at the University of Wollongong, working on an Australian Research Council (ARC)-funded project in the field of location-based services regulation. Roba is a lecturer and tutor in the Faculty of Informatics, teaching "Organisational Issues and Information Technology", and also holds the position of Solutions Development Manager at Internetrix, an interactive website development company. Ms Abbas has previously been involved in research centered on critical infrastructure protection (CIP), with a particular focus on the impact of public data availability on CIP efforts in Australia, and has presented related findings at a number of Australian workshops. Her honours thesis is available at http://ro.uow.edu.au/thesesinfo/2/. ra75@uow.edu.au

Dr Anas Aloudat recently completed his PhD in the School of Information Systems and Technology at the Faculty of Informatics at the University of Wollongong. His thesis investigated the utilisation of a nationwide location based service for emergency management within Australia. Dr Aloudat also holds a Master of Science in Computing from the University of Technology, Sydney. He is presently a sessional tutor and research assistant at the University of Wollongong. He is a member of the IEEE Society on Social Implications of Technology, a member of the Cellular Emergency Advisory Service Association, a member of the Disaster Preparedness and Emergency Response Association, and has been a member of the Research Network for a Secure Australia since 2006. He is also a reviewer of the Journal of Theoretical and Applied Electronic Commerce Research (JTAER). anas@uow.edu.au

Mr David Aspland is a lecturer with Charles Sturt University based at the School of Policing Studies at the New South Wales Police College in Goulburn, New South Wales, Australia where he currently specialises in Police Professional Ethics and researching Future Directions in Policing. He is former Inspector of the New South Wales Police who retired in early 2005 after 25 years of service. During that time he worked in both city and country locations in the roles of Constable, Shift Supervisor, Crime Manager and Duty Officer in a number of locations. He was attached to the NSW Police Academy from 1988 to 1997 working in the Police Recruit Education Program, the School of Organisation and Management Studies and the Intelligence Training Unit. He holds a Masters Degree in Public Policy and Administration from the Australian Graduate School of Police Management, Charles Sturt University. He is currently undertaking a PhD in Criminology at Griffith University through the Centre for Excellence in Policing and Security (CEPS) looking at the ethical issues that underpin public/private partnerships in policing and the interaction between the public and private policing sectors. He served in the Australian Army, both Regular

and Reserve, for over 8 years and was a Commissioned Officer in the Army Reserve serving as an Infantry Platoon Commander and Regimental Intelligence Officer. He has been a Member of the Australian Institute of Professional Intelligence Officers (AIPIO) since 1996, Police Futurists International (PFI) and the Board of Directors of the US based Public Safety Leadership Development Consortium (PSLDC) since 2007. His personal research and hobby interests centre on New South Wales Police history, badges and uniforms. On this range of topics he has written a number of articles for interest journals and is Assistant Secretary of the Police Insignia Collectors Association of Australia (PICAA).

Professor Simon Bronitt is the Director of the Australian Research Council Centre of Excellence in Policing and Security (CEPS). Before joining Griffith University in 2009, he was a Professor of Criminal Law in the College of Law at the ANU (1991-2009). During that time, he was also the Director of the EU-funded research centre, The National Europe Centre (2003-2009). He has held numerous visiting positions in North America, Hong Kong and Europe. His principal publication is S Bronitt and B McSherry, *Principles of Criminal Law* (3rd ed 2010 Thomson Reuters), and has published widely on the topic of surveillance, covert policing and human rights.

Mr David Chadwick is based in Canberra, Mr. Chadwick is responsible for working with Unisys delivery teams to develop and implement world class identity management solutions that achieve customer objectives and meet their business needs. David works with clients to assist them to understand the benefits that enhanced identity management solutions can deliver for them in their everyday business. Prior to joining Unisys in August 2007 Mr. Chadwick worked at the Australian Department of Immigration and Citizenship (DIAC) in a variety of roles including Director – IT Continuity Management, Airline Liaison Officer – Taiwan, Biometric Specialist and Business Analyst. During his time at DIAC he worked in the field of biometrics and imaging standards and was actively involved with the initial biometric capture trials in 2004-05. He also developed the department's facial imaging guidelines. Mr. Chadwick has over 18 years of law enforcement experience, having served with the South Australia Police (sworn) and the Australian Federal Police (un-sworn). He has extensive experience in all aspects of technical imaging, with 9 years experience in forensic and surveillance imaging. Mr. Chadwick has also performed consultancy work with a number of Government agencies in the field of digital imaging and image enhancement since 1997. He is the co-author of the "Australasian Guidelines for Digital Imaging Processes" for the Senior Managers Australian and New Zealand Forensic Laboratories, and the co-inventor of the world's first computer-based facial identification system in 1988. Mr. Chadwick has an Advanced Certificate (Diploma level) of Commercial Photography, and is a Certified Biometric Security Professional and Biometric Security Engineer. He also holds ITIL Foundation Level Certification. Since 2003 he has taught Advanced Forensic Technical Photography at the Canberra Institute of Technology.

Professor Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the UNSW, a Visiting Professor in the E-Commerce Programme at the University of Hong Kong, and a Visiting Professor in the Department of Computer Science at the Australian National University. He was for a decade the Chair of the Economic Legal and Social Implications Committee of the Australian Computer Society, and spent some time as the ACS Director of Community Affairs. He holds degrees from UNSW and ANU, and has been a Fellow of the ACS since 1986. He has been a Board-member of the Australian Privacy Foundation since its foundation in 1987, and its Chair since 2006. He has undertaken research, consultancy and public interest advocacy, and published extensively in Australia and overseas for over 30 years, in the areas of identification, security, dataveillance and social impacts and implications of information technology. His website is one of the most extensive and most used resources in these areas. Roger.Clarke@xamax.com.au

Mr Jeff Corkill is a Lecturer at Edith Cowan University in Perth where he lectures in Intelligence and Security. Jeff is a former Army Intelligence Officer who after twenty years in the military made the move to the private sector in 1998. Jeff has held a number of security management roles in the resource sector and consults in the security and intelligence field. His previous consultancy work has included working with the UN and the Government of Sierra Leone to establish a specialist diamond sector policing capability. His PhD research is exploring the concept of Professional Intelligence Judgement within the law enforcement context. His additional research interests are in the areas of human factors analysis and intelligence as an aid to CCTV surveillance operations and intelligence analysis particularly source and information evaluation.

Mr Adam Goodall LLB(Hons) BCom is the Director Inspections within the Office of the Commonwealth Ombudsman. He is responsible for managing a program of inspections and reporting requirements for the Commonwealth Ombudsman under the Telecommunications (Interception and Access) Act 1979, Surveillance Devices Act 2004, Part 1AB of the Crimes Act 1914, Crimes (Controlled Operations) Act 2008 (ACT) and Crimes (Child Sex Offenders) Act 2005 (ACT), and for co-ordinating input from the Ombudsman's Office on policy development matters relating to the oversight of law enforcement agencies and their use of covert and coercive powers.

Dr Clive Harfield is an Associate Professor in the Faculty of Law, University of Wollongong. His research interests focus on laws in relation to police governance, the regulation of covert investigation and the processes of transnational criminal investigation.

Mr Peter Mahy is a solicitor and a partner at Howells and the Head of the Civil Liberties department. He has an honours law degree from Sheffield University and a Masters in Criminology from the University of Cambridge. He completed his Legal Practice Course at the University of Northumbria, Newcastle. He joined Howells in 1996, qualifying in 1998.

Associate Professor Katina Michael (MIEEE'04, SMIEEE'06) holds a Doctor of Philosophy in Information and Communication Technology (ICT) from the Faculty of Informatics at the University of Wollongong, NSW, Australia ('03); a Master of Transnational Crime Prevention from the Faculty of Law at the University of Wollongong ('09) and a Bachelor of Information Technology from the School of Mathematical and Computing Science, NSW, Australia at the University of Technology, Sydney ('96). She is presently an Associate Professor at the University of Wollongong in the School of Information Systems and Technology ('02-'11) in Australia, and has previously been employed as a senior network engineer at Nortel Networks ('96-'01). She has also worked as a systems analyst at Andersen Consulting and OTIS Elevator Company. Michael has published several edited books, but more recently co-authored a 500 page reference volume: Innovative Automatic Identification and Location Based Services: from Bar Codes to Chip Implants (Hershey, PA: IGI, 2009). She has published over 85 peer reviewed papers. Michael researches predominantly in the area of emerging technologies, and has secondary interests in technologies used for national security and their corresponding social implications.

Dr M.G. Michael Ph.D, MA(Hons), MTh, BTh, BA is a theologian and historian who brings a unique perspective on Information Technology and Computer Science. Presently he is an honorary senior fellow in the School of Information Systems and Technology, at the University of Wollongong, Australia. He is the former coordinator of Information & Communication Security Issues and since 2005 has guest-lectured and tutored in Location-Based Services, IT & Citizen Rights, Principles of eBusiness, and IT & Innovation. He has presented papers at numerous IEEE conferences including the *International Conference on Mobile Business, the International Conference on Mobile Computing and Ubiquitous Networking, and RFID Eurasia*. In 2007 he was invited to deliver a paper at the *29th International Conference of Data Protection and Privacy Commissioners* (ubiquitous computing track) in Canada. He has co-authored a book titled, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants* and is credited with coining the term uberveillance which in 2009 entered the Macquarie Dictionary in Australia. Michael is currently working on an edited volume titled: "Uberveillance." Michael has been the recipient of a number of scholarships and awards. He is a member of the American Academy of Religion. mgm@uow.edu.au

Associate Professor Nick O'Brien represented the UK Association of Chief Police Officers - Terrorism and Allied Matters Committee (ACPO-TAM) and all the UK police forces as the Counter Terrorism and Extremism Liaison Officer (CTELO) at the British High Commission in Canberra, before joining Charles Sturt University. Nick covered Australasia and had a 'watching brief' on the Asia and the Pacific region. Prior to this posting Nick was in charge of International Terrorism Operations in Special Branch at New Scotland Yard. He also had responsibility for the National Terrorist Financial Investigations Unit (NTFIU) and International Liaison. Nick has

had national responsibility for all Special Branch training in the United Kingdom. Nick represented the UK at the G8 Counter Terrorist Practitioners Meetings and was the author of the G8 paper on 'Best Practices in Dealing with Suicide Terrorism'. Nick has visited both Sri Lanka and Israel to study the phenomenon of suicide attacks. Nick has also represented the UK at Europol and the European Police Working Group on Terrorism. Nick has spoken on Counter Terrorism at Conferences in Europe, New Zealand, Australia, Singapore, Thailand, Canada, Fiji, Tonga, Vanuatu and Malaysia. Nick has also visited a number of countries on terrorist related matters: France, Holland, Poland, the Czech Republic, Italy, Southern Ireland, Indonesia, Greece, the United States, Canada, Israel, Sri Lanka, Singapore, Malaysia, Papua New Guinea, Fiji, Tonga, Vanuatu, Thailand, the Philippines as well as Australasia. Nick first started working in the counter terrorism related area in 1981 and has worked on Irish as well as international terrorism. Academically Nick has a Post-Graduate Diploma in Personnel Management and a Master of Arts in Human Resource Management

Mr Rob Nicholls is an independent consultant who previously worked with Gilbert + Tobin. He has been a communications specialist for 25 years focusing on technology, regulatory and business strategy in broadcasting and telecommunications. He has an extensive technical and regulatory background which he combines with commercial, finance and analytical experience. He has been widely published and was a regular presenter at local and international conferences in the fields of regulation, telecommunications and broadcasting. Rob has an honours degree in Electronics and Communications Engineering from Birmingham University and a Master of Arts in International Relations at UNSW. He is currently a PhD candidate at UNSW in the field of the global politics of the regulation of broadcasting. Since the submission of his paper, Rob has moved on, now working at the ACCC and *doing* regulation, not just writing about it.

Dr Lucy Resnyansky, Research Scientist, Command, Control, Communications & Intelligence Division (C3ID), (DSTO), Australia. She has a PhD in Social Philosophy (1994) from Novosibirsk State University (Russia) and a PhD in Education (2005) from the University of South Australia. Her research experience covers studies of language as an instrument of power and influencing public opinion; computer-mediated communication; and discourse analysis of multimodal texts. Current research interests are in the areas of social modelling, epistemological aspects of multidisciplinary research, cross-cultural communication, sociocultural implications of technology, and use of ICT-mediated information sources. These issues are approached from the perspective of sociology of science, philosophy of technology, activity theory, semiotics and discourse theory. Lucy.Resnyansky@dsto.defence.gov.au

Dr Mark Rix is a Senior Lecturer in the Business School at the University of Wollongong. His research interests are in the areas of access to justice, human rights and the rule of law, and counter-terrorism and liberal democracy. mrix@uow.edu.au

Notes