# BALANCING PRIVACY AND SECURITY IN THE AUSTRALIAN PASSPORT SYSTEM

## STEVEN R CLARK*

*Passports are government-issued identification documents. They provide evidence of identity and citizenship, facilitating international travel and national security measures. This places them at the centre of debates regarding the balance between an individual's privacy and the security of the community. Understanding the technologies used to implement passport systems can shift the discussion from privacy versus security, towards privacy and security — enhancing both. This article reviews these issues from the perspective of existing laws and future policy-making.*

## I INTRODUCTION

Contemporary passports have ancient antecedents, but their current form came into existence in the 1920s through the influence of the League of Nations.[1] After the Great War, nations began to require 'documentary substantiation of identity used to register and keep watch over aliens'.[2] By 1929, the passport had become standardised, along with an increasingly bureaucratised and securitised regime of population movement.

The document has evolved over the past century, along with changes in international relations and shifts in the security interests of nations. New technologies have been exploited to increase the security and reliability of these documents as a means to verify identity. Australia's current passports and passport laws are no exception, indeed Australia has been an active

* BSc (Hons), LLB (Hons) (Flinders), MACS CP, MIEEE, Barrister and Solicitor of the Supreme Court of South Australia, PhD Candidate, University of South Australia. The author would like to thank Professor Rick Sarre, University of South Australia, and the anonymous referee, for their valuable comments on the draft of this article.

[1] Jane Doulman and David Lee, *Every Assistance & Protection: A History of the Australian Passport* (Federation Press, 2008) 91.

[2] John Torpey, 'World War One and the Birth of the Passport System' in Jane Caplan and John Torpey (eds), *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press, 2001) 269–70.

participant in the development and implementation of international passport standards.

From the 1960s onwards, with rising numbers of citizens travelling by air, automation of passport processing became increasingly attractive. In 1978 the international community settled a standard for a new Machine Readable Passport (MRP).[3] An active participant in the MRP program, Australia implemented this standard in 1983, introducing one of the first machine readable passports.[4]

It was these 1983-style Australian passports that were compromised as part of the assassination of Hamas' Mahmud Abdel Rauf al-Mabhuh in Dubai on 20 January 2010. The Australian passports of Nicole Sandra McCabe, Adam Marcus Korman and Joshua Daniel Bruce were used by members of the Israeli Secret Service team to enter Dubai.[5] Investigations by the Australian Federal Police (AFP) and the Australian Passport Office (APO) soon established that the three Australian passports had either been duplicated or altered.

The Foreign Minister, Stephen Smith, was quick to reassure Australians that the security of Australian passports had improved significantly since 2003, when these passports had been issued.[6] Several persons came forward at the time, claiming that Israeli agents had used Australian passports many times prior to January 2010,[7] and that the Australian government had ignored their warnings.[8] Both claims were denied by the Australian government.[9]

---

[3] International Civil Aviation Organisation, *Doc 9303: A Passport with Machine Readable Capability* (1980).

[4] Doulman and Lee, above n 2, 192–3.

[5] Ronen Bergman, 'The Dubai Job', *GQ* (online) January 2011 <http://www.gq.com/news-politics/big-issues/201101/the-dubai-job-mossad-assassination-hamas>.

[6] Joe Kelly, 'Australian Passports in Hamas Hit Duplicated or Altered, Stephen Smith Says', *The Australian* (online), 25 February 2010 <http://www.theaustralian.com.au/news/australian-passports-in-hamas-hit-duplicated-or-altered-stephen-smith-says/story-e6frg6n6-1225834232594>.

[7] 'Israeli Spy Agency Mossad Regularly Faked Australian Passports: Ex-Agent', *The Sydney Morning Herald* (online), 26 February 2010 <http://www.smh.com.au/national/israeli-spy-agency-mossad-regularly-faked-australian-passports-exagent-20100226-p8om.html>.

[8] Mark Dodd and Paul Maley, 'Warning on Passport Forgery Ignored, Says Former Diplomat', *The Australian* (online), 26 February 2010 <http://www.theaustralian.com.au/national-affairs/defence/warning-on-passport-forgery-ignored-says-former-diplomat/story-e6frg8yo-1225834538957>.

[9] Ibid.

Nevertheless, the older MRP documents are easily compromised. On 1 July 2010, Victoria Police raided a house in the Melbourne suburb of Brooklyn as part of an ongoing investigation into an alleged 'war' between two rival crime families. They uncovered firearms, ammunition, and more than thirty blank passports on the property. Members of the Chaouk family were charged with related offences.[10]

When it introduced its new biometric passport in 2005, the Australian government hailed it as an improvement upon the original MRP documents.[11] Biometric passports were commended for being more difficult to counterfeit, better integrated with passport databases, and for enabling a broader range of data interactions. The biometric passport has features that make it significantly more secure than previous passports, but also a greater threat to privacy.

This article examines the key legal and technological milestones in the recent history of the Australian passport. The emphasis in the 1970s was on the application of technologies to improve the flow of international passengers. A series of royal commissions into drug smuggling shifted this emphasis in the 1980s to improving the integrity of the passport issuing process. The Machine Readable Passport enabled, for the first time, a direct link between a physical passport document and an electronic record of the facts relating to it. This tightened the security of the passport system, and enhanced its potential usefulness to law enforcement internationally.

The possibility of expanding this connection to enable real-time identification of persons-of-interest via their use of their passports as they travel was viewed as the next logical step. However, it would not be until the first years of the twenty-first century that the technological means to 'physically' connect a traveller with their passport (via a biometric), and thus to an electronic record, became feasible. This coincided with a marked increase in national security concerns following the events of 11 September 2001. This confluence of events raises some important questions regarding the relative value placed upon privacy and security within new biometric passport systems.

---

[10] Elissa Hunt, 'More Charges for Chaouk Brothers', *Herald Sun* (online), 26 August 2010 <http://www.heraldsun.com.au/news/victoria/more-charges-for-chaouk-brothers/story-e6frf7kx-1225910418826>; Elissa Hunt, 'Omar Chaouk, Held after Police Raid on Brooklyn Home, Freed on Bail', *The Herald Sun* (online), 12 July 2010 <http://www.heraldsun.com.au/news/omar-chaouk-held-after-police-raid-on-brooklyn-home-freed-on-bail/story-e6frf7jo-1225890728582>.

[11] Department of Foreign Affairs (Cth), 'Australia Launches ePassports' (Media Release, 25 October 2005) <http://www.foreignminister.gov.au/releases/2005/fa132_05.html>.

## II THE INTRODUCTION OF MACHINE READABLE PASSPORTS

A false passport was an essential prerequisite to a drug smuggling career in the 1970s. Passengers and goods were subjected to an elaborate and expensive customs screening process. This process utilised a watch-list of names, and a general suspicion of anyone who travelled to, or through, drug-producing regions. The screening process was also important in interdicting a range of criminal activities beyond drug smuggling, including terrorism, illegal immigration, and evasion of health and quarantine restrictions. This regime was easily circumvented by Australians travelling on fraudulently obtained but valid passports.[12]

The Australian Royal Commission of Inquiry into Drugs (ARCID) ('the Williams Royal Commission') was established in October 1977 to investigate the importation and trafficking of illegal drugs and the connections between drugs and other organised crime in Australia. In its report, the Commission estimated the number of heroin addicts in Australia at the time to be between 14200 and 20300 persons.[13] The main sources of the drugs were the Golden Triangle (Thailand-Burma-Laos), the Golden Crescent (Afghanistan-Pakistan-Iran), and the Bekka Valley of Lebanon. Almost all the heroin on sale in Australia was arriving by air, carried by drug couriers in kilogram quantities.[14]

This was made possible by the use of multiple and false passports. The use of false passports was well known, with several significant cases widely reported in the years prior to the Williams Commission. The Commission's final report included several recommendations regarding passport applications: that they should be made in person; and that procedures for the identification of applicants and the provision of birth certificates should be changed.[15]

These findings prompted the then Prime Minister, Malcolm Fraser, to establish a special judicial enquiry with the powers of a royal commission.[16] On 25 June 1981, the Commonwealth, Queensland, Victorian and New South

---

[12] Commonwealth, Royal Commission of Inquiry into Drug Trafficking, *Passports: Interim Report No 2* (1982).

[13] Commonwealth, Australian Royal Comission of Inquiry into Drugs, *Report* (1980) D7.

[14] Doulman and Lee, above n 2, 195–6.

[15] Australian Royal Commission of Inquiry into Drugs, above n 13, B279 (Recommendations 89, 90, 91 and 93) and D102, referred to by Commissioner Stewart in Royal Commission of Inquiry into Drug Trafficking, above n 12, 14–15.

[16] Doulman and Lee, above n 2, 196.

Wales governments established the Royal Commission of Inquiry into Drug Trafficking. Justice Donald Stewart of the NSW Supreme Court was empowered to inquire into the drug trafficking and associated activities of Terrance John Clark and his associates. In particular, the Commissioner was to inquire into their 'nature and extent', 'the identity and involvement of [associated] persons', their 'methods of operation' and their use of 'banking, financial and other institutions'.[17] Also of interest was whether Clark or his associates obtained information from government officials, or interfered with the course of justice.[18]

The Stewart Royal Commission of Inquiry into Drug Trafficking (Stewart Royal Commission) spent much of its time examining how criminals were abusing the Australian passport system. Justice Stewart set out the scale of the abuse of the system in detail in *Interim Report No 2*,[19] presented to the Governor-General and the Governors of NSW, Queensland and Victoria on 17 May 1982.[20]

### *A False Passports*

False passports generally only come to light when the bearer is charged with a serious offence. This has always been the case. Neither the Department of Foreign Affairs (DFA), the Department of Immigration and Ethnic Affairs (DIEA) or the Australian Federal Police (AFP) were able to provide details to the Stewart Royal Commission regarding the number of false Australian passports discovered by any of the agencies.[21]

When questioned by the Stewart Royal Commission, the DFA argued in its defence that its primary concern was the issuing of genuine passports, and that it was not involved in the investigation of fraudulent passports. The Department had no information regarding the numbers of fraudulently altered passports, the nature of any alterations, nor the numbers of counterfeit passports detected. The DIEA was also unable to furnish the Stewart Royal Commission with information from the time it had administered the passport

[17] Ibid 97.
[18] Ibid 98.
[19] Ibid.
[20] Doulman and Lee, above n 2, 196.
[21] Royal Commission of Inquiry into Drug Trafficking, above n 12, 43.

system.[22] It also became apparent that there had been a lack of communication between the departments and law enforcement agencies.

The use of fraudulently obtained passports by drug smugglers had been identified as early as 1966, when three former NSW police officers, John Wesley Egan, Harry Ikin and Murray Stewart Riley, were caught smuggling heroin from South East Asia into Australia and the USA.[23] By the time Commissioner Williams began taking evidence for ARCID ten years later, the practice had become more common. Commissioner Stewart was in no doubt that it was even more widespread by the time he began his inquiry in 1981.[24]

### *B Samir Makary*

Commissioner Stewart became so concerned about failures to address the availability of false passports that he devoted his second interim report to the subject. To illustrate the depth of the problem, he recounts the following story of Samir Makary.[25] Makary had come to the attention of the Royal Commission, and had been identified in the Commission's first interim report. Nevertheless, Makary was able to evade prosecution by obtaining a false Australian passport.

On 27 October 1981, police officers,[26] acting on the confidential first interim report of the Stewart Royal Commission, arrested Samir Makary, a Lebanese national, in Northmead in the western suburbs of Sydney. He had in his possession almost four hundred grams of what appeared to be high grade heroin. A similar quantity of the drug was found at his Granville home. Chemical analysis later confirmed that Makary was in possession of 743.9 grams of 52 per cent pure heroin of Middle Eastern origin.[27]

Makary appeared before the Chief Magistrate of New South Wales at Sydney on 28 October 1981. Bail was refused in the first instance, but this was overturned on appeal by Mr Justice Yeldham of the Supreme Court of New

---

[22] The DIEA was also unable to furnish an answer to either the Minister for Foreign Affairs nor the Minister for Immigration and Ethnic Affairs. For example, see question on notice in Commonwealth, *Parliamentary Debates*, House of Representatives, 28 May 1981, 2859 (Tony Street, Minister for Foreign Affairs).

[23] Royal Commission of Inquiry into Drug Trafficking, above n 12, 43.

[24] Ibid 41–7.

[25] Ibid 41–2.

[26] Members of the Commonwealth–State Joint Task Force on Drug Trafficking, assisted by the New South Wales Police Drug Squad and Air Wing.

[27] Royal Commission of Inquiry into Drug Trafficking, above n 12, 41.

South Wales. Bail was set at $75 000, with the conditions that Makary surrender his passport, not approach international airports, and report to the Granville police station every morning and evening.

On 4 December 1981, Makary pleaded guilty before a magistrate and was committed for sentencing by the District Court of New South Wales on 18 December 1981. The prosecution failed to apply for review of his bail, allowing him to walk out of the court. Makary's counsel appeared on his behalf at the December 18 hearing, informing the court that Makary was in hospital. Judge Cameron-Smith remanded Makary to appear before the Court on 15 January 1982, and ordered the issue of a warrant to lie in the Court office, to be executed should he not appear.

On 15 January 1982, Makary's counsel again appeared on his behalf, this time to advise Judge Ward that he had no further instructions. Police immediately sought to execute the warrant, but without success. Makary had last reported to the Granville police station on the morning of 13 January 1982. He left Australia just after midday the same day on a Yugoslavian aircraft, heading to Damascus via Dubai.[28]

When police searched Makary's home, they found six passport-sized photos of him in a packet. The photographer recalled taking eight photos of Makary in late December 1981 or early January 1982. Five police officers then began manually searching through the 15 000 passport applications made at the Sydney Passports Office between 1 December 1981 and 15 January 1982. They eventually discovered an application with Makary's photograph attached.

Makary had applied for a passport on 23 December 1981 in the name of Kevin William Harris, date of birth 18 July 1951. The application listed William Harris, of 44 Brain Avenue, Lurnea, as the father. A passport was issued on 4 January 1982, and collected by a travel agent on 12 January.

Police obtained a birth certificate for Kevin William Harris who was born on 18 July 1951. They also obtained a death certificate dated 16 August 1952, which indicated that he had died aged less than 13 months. They learned that an earlier application for a copy of the birth certificate had been made in the name of William Harris, as the father of Kevin William Harris, claiming it was required for probate purposes. That application was accompanied by a typewritten letter authorising an Alfred Wilhelm Gruner to collect a birth certificate on behalf of William Harris. Gruner proved to be an entirely fictitious alias. The letter was well phrased, and the handwriting on the

[28] Ibid 42.

document was similar to the signature of the travel agent on similar documents regarding arrangements to collect Makary's false passport.[29]

The passport application also included a certificate of identity endorsed by a William Victor Cook, JP, bank officer, retired. The telephone book listed a WV Cook JP. When Wilfred Vincent Cook JP, stock and station agent, was interviewed by police, he stated that he had no knowledge of the matter. It was assumed that his name had been selected from the phone book because of the 'JP' suffix.

Police also visited the Church of England cemetery at Woronora where Kevin William Harris's death certificate indicated he had been buried. His burial was marked by a simple wooden cross without inscription. It was clear that Makary had not obtained Kevin William Harris's details from the cemetery. This avenue of inquiry was suggested by Frederick Forsyth's 1971 novel *The Day of the Jackal*, which had been made into a movie in 1973. In the novel (set in 1963), the eponymous character 'The Jackal' is an assassin hired to kill Charles de Gaulle, then President of France. He acquires a false passport by visiting a cemetery and applying for the birth certificate of a deceased child, using details from the child's gravestone. This is then used to apply for a passport in the child's name.

The 32 year old Lebanese national, who had arrived in Australia less than 10 years earlier, was able to obtain an Australian passport upon claiming to have been born in Australia 30 years previously to William Harris and Lorna Harris. The Passports Office at the time was more concerned with protecting the privacy of applicants and providing a timely and convenient service than securing the process from abuse. Makary was just one in a long line of criminals (and others) reaching back at least to the 1960s who had been able to obtain a valid, but false, Australian passport.

## III REFORMING PASSPORT LAW AND PROCESSES

In the thirty years following the introduction of the *Nationality and Citizenship Act 1948* (Cth), Australians could get a passport on proof of citizenship and proof of identity. Citizenship could be proved by a birth certificate or certificate of naturalisation. Proof of identity was furnished by a

[29] Ibid.

Certificate Regarding Applicant (CRA), signed by a qualified person,[30] certifying that the two photos supplied with the application were photos of the applicant. Prior to the Stewart Royal Commission, information supplied to passport issuing officers by applicants — or 'certifiers of identity' — was rarely independently verified.[31] Indeed, it was a widely held opinion amongst government officials (including AFP officers), that many travel agents and passport applicants regarded the CRA to be 'a joke'.[32]

During the 1970s, increasing computerisation had improved passport issuing processes. In 1976, passport records which had been held at state offices were centralised, making it easier to cross-check applications. Index card records were computerised in 1978. By 1980, every passport-issuing officer in Australia had online access to a central computer, preventing the issue of passports with the same name and date of birth as one already issued.[33]

However, prior to the implementation of the Stewart Royal Commission reforms, only a third of applications were made at Passport Offices in person. The other two thirds were made by mail or on behalf of the applicant by travel agents (and others). Stewart reflected on the irony of tax payers funding expensive systems designed to prevent criminality, while at the same time funding a passport system that readily enabled criminals to circumvent those very systems with impunity.[34]

The Stewart Commission uncovered three methods used to obtain a false passport:[35]

1. Application using the birth certificate of a deceased person;

2. Application using a borrowed, bought or stolen birth certificate of a living person;[36]

---

[30] Qualified persons included magistrates, justices of the peace, solicitors, accountants, medical practitioners, chartered engineers, members of parliament, union officials, bank managers, teachers, and managers.

[31] Royal Commission of Inquiry into Drug Trafficking, above n 12, 63.

[32] Doulman, above n 2, 197–8.

[33] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 1982, 3079 (Tony Street, Minister for Foreign Affairs).

[34] Royal Commission of Inquiry into Drug Trafficking, above n 12, 4X and again in Donald Stewart, *Recollections of an Unreasonable Man: From the Beat to the Bench* (ABC Books, 2007) 157–8.

[35] Doulman and Lee, above n 2, 198–9. These three summarise the five methods reported by the Commission.

3. Collusion with an officer in the Passport Office, who would remove the physical file regarding the application after the passport was issued.

The Passport Office retained documentation for each passport application and passport issue: the application form; a check sheet; the application's second photo (the first being attached to the passport); a register of passport numbers; the name of the person to whom the passport was issued; and other particulars. If this 'dossier' were removed from the files, the Office had no other record of how the valid passport came to be issued. Thus, if questioned, the Office could only confirm that the passport had been issued.[37]

Sir Edward Williams's Australian Royal Commission of Inquiry into Drugs (ARCID) had recommended only a few years earlier that passport applicants ought to present in person to a Department of Foreign Affairs (DFA) office.[38] The DFA considered this impractical. With two thirds of applications made by mail or via an agent, the proposal would add 274 000 applicants to the 148 000 who had presented themselves during 1979 alone. 'The Stewart Royal Commission doubted whether the department appreciated the scale of the abuse of the system that was taking place.'[39]

The DFA argued that the increased volume of applications would mean that documents could receive only the briefest of scrutiny by officers. Most documents of identity were beyond the Department's control, and were readily available. False documents presented for a passport application would pass casual scrutiny with little difficulty. But this position taken by the DFA dismissed the possibility that checks could dissuade some from attempting fraud, and might catch others who made an attempt.

The Stewart Royal Commission set out 40 recommendations for reforms to the passport system to improve its integrity and security. In particular it recommended that:

---

[36] This was risky unless you knew the person would never, and had never, applied for a passport.

[37] Doulman and Lee, above n 2, 199.

[38] The ARCID Recommendation 89 reads: 'As a general rule, applicants for passports should be required ... to present themselves in person at an office of the Department of Foreign Affairs and to produce there any supporting documentation required to satisfy the issuing officer as to their identity': quoted by Royal Commission of Inquiry into Drug Trafficking, above n 12, 15.

[39] Doulman and Lee, above n 2, 200. See also Royal Commission of Inquiry into Drug Trafficking, above n 12, 41: 'This Commission has grave doubt as to whether the Department really appreciates how serious the present position is.'

- Applicants should apply at a Passport Office in person, unless exempted;
- Passports only be issued to Australian citizens;[40]
- Birth certificates alone no longer be accepted as sufficient proof of identity;
- Passports no longer be issued to travel agents or other agents.

It also recommended:

- The establishment of a Passports Committee as an interdepartmental standing committee to supervise the security of Australian Passports and visas, and other passports and documents used to enter Australia;
- The introduction of legislation in each State requiring the registration of any change of name (whether by choice, marriage, or adoption) with the relevant Registrar of Births, Deaths and Marriages (RBDM); and
- The upgrading of the classification of the staff in the Passports Office, and their office accommodation.[41]

In response, the DFA established an internal working party to assess the options available for processing passport applications and issuing travel documents. The Department also established a Passports Committee to advise the Minister. The DFA provided the chair, with other members drawn from the Customs Service; the Australian Federal Police (AFP); the Attorney-General's Department (AGD); the Postal Commission; the Australian Government Publishing Service (AGPS); the Australian Bureau of Criminal Intelligence (ABCI); the Department of Immigration and Ethnic Affairs (DIEA); and the Department of Prime Minister and Cabinet (DPMC).[42]

There were criticisms within the DFA that the Stewart Royal Commission had not considered the full picture. J R Kelso, former Director of Passport Operations, wrote in an internal document:

---

[40] British subjects, regardless of nationality, until that time could apply for and be issued with an Australian passport.

[41] Royal Commission of Inquiry into Drug Trafficking, above n 12, 89–94.

[42] Doulman and Lee, above n 2, 201–2.

> Its observations on passports were those undertaken from what might broadly be described as a control and enforcement perspective. But there are other important factors to be taken into account in any examination of the passports function. These include, for example, the rights of citizens to travel and hence to obtain passports, *the extent to which it is appropriate to permit increased intrusions into privacy* and to create inconvenience for individuals, the staffing and costing implications, etc.[43]

This view was supported by I G Bowden, First Assistant Secretary of the Consular, Information and Cultural Division:

> The passport function can never be used as a mechanism for enforcement and control, but rather as a beneficiary of other control procedures.[44]

Another sticking point for the Department was Commissioner Stewart's proposal to create regional issuing agencies, outside the major cities. J A Benson, Assistant Secretary of the Executive Secretariat of the DFA was concerned that:

> [t]he recommendations make no reference to a balancing of the cost to society of these extra facilities against the expected social gain from what is likely to be no more than reduced ease of travel for drug traffickers.[45]

### *A National Identity System Proposal*

By 1982, the DFA considered that only a *national identity system* could deliver a robust passport system. But any such 'ID system would have to be based on physiological characteristics such as finger printing, cell testing, blood typing, voice recognition combined with registration of the residence of all those who reside in Australia'.[46] Of these, only fingerprinting could be reasonably automated using technologies available at the time. The strong association of fingerprinting with criminal processing would make this a 'hard sell'. Other available biometric technologies (such as cell testing or voice

---

[43] Minute from J R Kelso to I G Bowden, 5 July 1982 (National Archive of Australia: A1838, 1622/12/8/44 part 1) (emphasis added).

[44] Minute from I G Bowden, 13 August 1982 (National Archive of Australia: A1838, 1622/12/8/44 part 1).

[45] J A Benson, Minute from J A Benson to T B McCarthy, Assistant Secretary, Consular Policy Branch, 28 Jun 1982 (National Archive of Australia: A1838, 1622/12/8/3 part 1) (1982).

[46] Minute from J R Kelso to I G Bowden, 5 July 1982 (National Archive of Australia: A1838, 1622/12/8/44 part 1).

recognition) were time and resource intensive, and thus unsuitable for processing large numbers of applications, let alone timely immigration processing in concert with customs checks at entry points into Australia.

There was an additional problem. The ancestors of most Australians were not living in Australia, and there was no common system of registration of births, deaths and marriages across the states and territories.[47] Taken together, this meant that there was no existing reliable and interoperable benchmark for establishing identity — founded upon either the person themselves, their ancestry, or the provenance of their identification documents — with which to address identification issues.

The Department advised government ministers in July 1982 that any national identity system would be expensive to implement, difficult to administer, and likely to provoke political opposition.[48] However, the Department argued that, without one:

> it must be accepted that organisations which depend on securing the identity of people can never be sure that people cannot obtain benefits from government fraudulently and that determined people will be able to abuse the system. The Government in this case should accept that the passport system can never be perfect and should say so.[49]

The Minister for Foreign Affairs revisited the idea between 1985 and 1987, when the Hawke government proposed to introduce a national identity card for citizens and residents (the *Australia Card*). The card failed to win popular support and the idea was shelved. Had the Australia Card been introduced, the passport function may have been incorporated into a new Department of National Identity, along with other government identification systems to combat fraud in tax, health and welfare systems,[50] as it had been with the United Kingdom's Office of Passports and Identity twenty years later.[51]

---

[47] Doulman and Lee, above n 2, 202.

[48] Ibid 203.

[49] Note, 'Suggested Approach to Ministers to SRC Report on Passports', nd 1982 (National Archive of Australia: A1838, 1622/12/8/3 part 1).

[50] Doulman and Lee, above n 2, 206.

[51] The new Coalition government in the UK put dismantling the Identity Card system front-and-centre of its reform agenda, and has since done so.

### *B Passport Reforms*

On 8 December 1982, the Fraser government's Minister for Foreign Affairs, Mr A A (Tony) Street, announced that the government would address many of the Stewart Royal Commission's main criticisms, while largely accepting his Department's advice. He conceded that, whilst a national identity system based upon fingerprinting might be the most effective approach to addressing the shortcomings of existing identification processes, its 'implications on our traditional way of life' made it unattractive.[52]

The most significant change adopted by the government was to require applicants, from 1 October 1984, to attend in person before a passport officer. This would enable a trained officer to assess the identity documents and compare the photographs attached to the application with the applicant directly.

Rather than establish more Passport Offices and create more passport commissioners, post offices would act as agencies.[53] Post offices had several advantages: convenience for applicants; the fact that postmasters and senior postal clerks were already experienced in conducting interviews on an agency basis; the fact that post office staff could check the residential addresses of applicants; and the fact that the cost would be significantly less than establishing regional passport offices. Post office staff who handled an applicant's mail at local post offices could readily establish the applicant's *bona fides*. They could also cross-check passport applications and Certificates Regarding Applicants (CRAs) with electoral rolls, telephone directories, and other registers held at post offices.[54]

Additional identity checks were announced on 5 January 1982, including comparisons with electoral rolls and other records. The Department of Foreign Affairs began to contact applicants, and those certifying the applicant's identity, by mail or telephone. The Department also required the identity of all applicants to be checked as thoroughly as possible before a passport was issued.

---

[52] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 1982, 3079 (Tony Street, Minister for Foreign Affairs). Indeed such a radical programme was unlikely to assist Street, or the Liberals, at a future election.

[53] Ibid.

[54] Doulman and Lee, above n 2, 203–4.

The categories of persons able to certify the identity of applicants was restricted to:

> Members of Parliament — Federal and State; aldermen and councillors of municipal and shire councils; town clerks and secretaries; medical practitioners and dentists; judges, magistrates, clerks of petty sessions and clerks of court; school teachers of five years service; postmasters; police officers of the rank of sergeant and above and officers in charge of stations; officers of the armed services; ministers of religion designated as marriage celebrants; and Federal and State public servants of at least 10 years' permanent service.[55]

This was considered to be wide enough that applicants should know at least one person within any one category, and to include people whose *bona fides* could be readily checked by the Passport Office and whose careers would be affected by fraudulent conduct.[56]

Applicants were now required to provide a full birth certificate, showing their name at birth and the full names of both parents.[57] Photocopies of primary documents or birth extracts were no longer acceptable. In some states a person changing their name by Deed Poll could have a birth extract issued in their new name. To require a person's name at birth established a 'base name' for computer records.[58]

The government increased resources for passport functions to address sharply increasing demand. Between May 1982 and June 1985, passport applications increased by 30 per cent. Sixty per cent of applications were lodged at post offices, which were taking on much of the work previously handled by travel agents. Over the same period, Passport Office staff increased from 192 to 263, including 51 document and identity investigators, to carry out the additional checks, reporting and accountability measures associated with the Stewart reforms.

---

[55] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 1982, 3079 (Tony Street, Minister for Foreign Affairs). Conspicuously absent from this list were lawyers.

[56] Doulman and Lee, above n 2, 205.

[57] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 1982, 3079 (Tony Street, Minister for Foreign Affairs).

[58] This 'base name' was determined at the time of acquiring Australian citizenship: birth or naturalisation.

**Table 1: Number of Australian Passports issued between 1982 and 1985**

| Financial Year | Passports Issued[59] |
|---|---|
| 1982–1983 | 520 884 |
| 1983–1984 | 543 748 |
| 1984–1985 | 673 748 |

The reforms soon brought about measurable results. In 1985 the Australian Federal Police (AFP) reported a significant decrease in fraudulent passports amongst detained criminals as compared with previous years, especially those on drug charges.[60] A sub-committee of the Passports Committee examined 140 cases of Australians imprisoned overseas. Eighty per cent were imprisoned for drug offences. Many had a history of incidents regarding passports (including losing more than one). In each case, the DFA was able to contact the next-of-kin and confirm identity. In their comprehensive history of the Australian Passport, Jane Doulman and David Lee report that only one person had been able to obtain a passport under a false identity under the new procedures. That person had a history of mental illness, and had established a second identity over the previous two years.[61]

The Australian High Commission in Wellington reported three cases where the new procedures had prevented a passport being issued in the name of a false identity. A single instance of obtaining an Australian passport under a false identity was short lived. A temporary 20-day passport was issued in Brazil to replace one reported stolen. The application was soon discovered to be false, and the bearer arrested in Australia. The bearer was also found to be holding three other passports in their name.[62]

Commissioner Stewart was not convinced that the provision of consular services overseas was enough to require DFA administration of the passport system. He recommended that the passport function be transferred back to

[59] Figures from Doulman and Lee, above n 2, 205.

[60] Ibid.

[61] Ibid.

[62] Australian Passports Office, 'Review of Passport Procedures', internal departmental paper (1985).

DIEA,[63] arguing that the essential qualification for a passport was Australian citizenship, and thus the supply of passports ought to be administered by DIEA.[64] Some in the DFA supported the divesting of the passport function. However, the Consular and Passports Branch persuasively argued that Passport Offices were the public face of, and the only contact most Australians had with, the Department. Passport Offices were the 'single best opportunity [for] the Minister and the department ... to maintain a sympathetic constituency in Australia amongst Australians'.[65]

In 1986, the Department again successfully defended its administration of passports:

> [T]he passports organisation is more efficient than it ever has been and in large part we ascribe this to the intra-departmental relationships of passports, legal, consular and communications computers. Issue of passports is essentially part of our overseas function ... The passports database is now substantially improved, the incidence of disclosed malpractice is very low, and we believe it is the government's most accurate personal database.[66]

The tightening of controls surrounding the issuing of Australian passports significantly reduced misuse of the system. This not only improved the quality of the passport as a document for identification purposes; it also put in motion similar improvements to other identification documents. However, it also shifted the balance between privacy and security in the system in favour of security. This shift to an emphasis on security has accelerated since the events of 11 September 2001.

## IV INFLUENCE OF THE USA AFTER 11 SEPTEMBER 2001

Early on 11 September 2001 a group of Islamic terrorists affiliated with *al-Qaeda* hijacked four commercial airliners in the United States of America (USA). They flew two into the World Trade Center buildings in New York

---

[63] Recommendation: '38. While the determination of appropriate Commonwealth administrative arrangements is a matter for Ministers, the Commission is strongly of the view that Passport Offices should be part of the Department of Immigration and Ethnic Affairs and not part of the Department of Foreign Affairs': Royal Commission of Inquiry into Drug Trafficking, above n 12, 94.

[64] Ibid 70–3.

[65] Minute from R F Osborn (consultant), to J H Brook, First Assistant Secretary, Legal and Consular Division, 16 July 1985 (National Archives Australia: A1838, 1622/11/44 part 1).

[66] Minute from A D Campbell, Acting Secretary, to Bill Haydon, Minister for Foreign Affairs, nd 1986 (National Archive Australia: A1838, 1622/1/120 part 1).

City and one into the Pentagon Building. The fourth crashed in rural Pennsylvania — presumably heading to the White House. The World Trade Center buildings collapsed, and a total of 2973 people died.[67]

It was clear to many that terrorists were exploiting US immigration and border control mechanisms to operate inside the USA. Of the 48 foreign-born terrorists involved in plots between 1993–2001, 17 were naturalised US citizens or legal permanent residents; 16 were visiting on temporary visas; 3 made asylum applications; and 12 had crossed the US border illegally.[68]

The events of '9/11' changed the way many nations thought about national security. Their security thinking moved from an emphasis on defence against foreign national armies towards defence against global(ised) terrorism. This blurred the lines between 'internal' and 'external' security.[69] The desire for increased border protection measures and increased surveillance has had significant implications for passport systems worldwide.

During the 1990s, the dictum of 'out of sight, out of mind' was used to address most societal insecurities. But the clandestine entry of alien terrorists and the presence of sleeper cells in the 'homeland' are threatening because of their *invisibility*. They are a spectre lurking in the shadows. Security now seemed to require policies that *increased* visibility rather than *decreased* it so that the entry of potentially dangerous individuals could be prevented.[70] Consequently, airline passenger data, immigration records and passports, telephone and email logs all became the focus of government surveillance.[71]

In October 2001, Congress passed the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001* (USA PATRIOT Act).[72] This increased

---

[67] United States of America, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (2004) 552.

[68] Steven Camarota, 'How the Terrorists Get In' (2002) (149) *The Public Interest* 65, 67, drawing upon material from Steven Camarota, 'The Open Door: How Militant Islamic Terrorists Entered and Remained in the United States, 1993–2001' (Center for Immigration Studies, 2002).

[69] Christopher Rudolph, *National Security and Immigration: Policy Development in the United States and Western Europe since 1945* (Stanford University Press, 2006) 78.

[70] Ibid 79.

[71] David Lyon, *Surveillance after September 11* (Blackwell Publishing Ltd, 2003) 109.

[72] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Pub L No 107-56, 115 Stat 272 (2001).

several USA federal authorities' powers to carry out surveillance and to detain suspected terrorists; laid out additional grounds to refuse entry to those suspected of involvement in terrorism; and expanded the legal definition of terrorist activities to include 'material support' for terrorists or terrorist organisations. It also required the President, within two years, to certify a biometric technology standard to enable the identification of aliens seeking to enter the USA.[73]

The following year, the *Enhanced Border Security and Visa Entry Reform Act of 2002* (EBSVERA) was enacted. Amongst other provisions, it provided an additional incentive for international cooperation with a biometric standard:

> Not later than October 26, 2004, the government of each country that is designated to participate in the visa waiver program established under section 217 of the Immigration and Nationality Act shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with *applicable biometric and document identifying standards established by the International Civil Aviation Organization*.[74]

In order for its citizens to continue to be eligible for visa-free entry into the USA, Australia would have to develop and implement a biometric passport.

EBSVERA also led to an increase in the number of US immigration inspectors and investigators, and increased scrutiny of visa applications originating in countries suspected of supporting terrorism. A year after 9/11, the National Security Entry-Exit Registration System (NSEERS) was implemented under EBSVERA, requiring all foreign male visitors from 'politically sensitive' areas to register with authorities.[75]

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program superseded NSEERS, which was discontinued on 27 April 2011.[76] US-VISIT requires a digitally scanned fingerprint and a digital

---

[73] Ibid.

[74] *Enhanced Border Security and Visa Entry Reform Act of 2002*, Public Law 107-173, § 303(c)(1), 116 Stat 543, 554 (2002) (emphasis added).

[75] Doulman and Lee, above n 2, 209.

[76] US Department of Homeland Security, *Important NSEERS Information*, (20 May, 2011 <http://www.cbp.gov/xp/cgov/travel/id_visa/nseers/imp_nseers_info.xml> citing *Removing Designated Countries From the National Security Entry-Exit Registration System (NSEERS)*, 76 Fed Reg 23 830 (28 April, 2011).

photograph of all non-immigrant visa-holders. Their name and fingerprints are cross-checked with security databases before the visitor can enter the USA.[77]

The conditions imposed by the US for continued eligibility for its Visa Waiver Program (VWP) provided a significant impetus to countries such as Australia to develop and deploy a biometric passport. US-VISIT required that:

- Passports issued or renewed before 26 October 2005 must be machine readable;
- Passports issued or renewed after 26 October 2005 must be machine readable *and* contain a digitised photograph, or be biometric passports;
- Passports issued or renewed after 26 October 2006 *must* be biometric passports.

Visitors to the USA bearing passports which did not meet the relevant VWP criteria faced fingerprinting and other potentially invasive requirements before being allowed to pass passport control.

## V DEVELOPING A BIOMETRIC PASSPORT

The changes to US passport and immigration laws and procedures introduced following 11 September 2001 increased the momentum within the International Civil Aviation Organisation (ICAO) to settle upon a biometric passport standard. In fact, a Technical Working Group comprising representatives from Australia, Canada, the Czech Republic, France, Germany, India, Japan, New Zealand, the Netherlands, the Russian Federation, Sweden, the United Kingdom, and the USA had been researching an appropriate standard since 1995.[78]

Traditional passports contain a simple recognition detail: a photograph. However, people are not good at comparing multiple pairs of similar-looking people with photographs. Various technologies have been, and are being, developed to replace fallible humans with machines. Biometric passports have

---

[77] Christopher Rudolph, *National Security and Immigration: Policy Development in the United States and Western Europe since 1945* (Stanford University Press, 2006) 80.

[78] Doulman and Lee, above n 2, 210.

all the features of traditional passports, supplemented with a computer file incorporating 'commonly known personal attributes (name, date of birth, sex and so on) and biometric data to enable machines to verify the identity of the passport holder'.[79]

Identity verification is generally reliant upon one of three processes. The first is the possession of a document (*what you have*) such as a driver's licence, passport, or credit card; but these could be fraudulently obtained, stolen, lost, or used to create a false identity. The second is the possession of knowledge (*what you know*), such as a password or secret; though if it were too short or too simple, it might be easy to guess/crack, and if too long or too complex, too difficult to remember. The third is the use of biometrics: using a person's own body (*what you are*) as validation of identity. This would generally be difficult to forge. Examples of biometric validation include comparison of fingerprints, facial recognition, hand geometry, and iris recognition.

For the ICAO, biometric passports serve two main purposes:

> *Verification* — 'confirming identity by comparing identity details of the person claiming to be a specific individual against details previously recorded on that individual'; and
>
> *Identification* — 'determining possible identity by comparing identity details of the presenting person against details previously recorded on a number of living individuals'.[80]

Seven criteria were used by the ICAO to assess available technologies:

1. Compatibility with enrolment requirements;
2. Compatibility with Machine Readable Travel Documents (MRTD) renewal requirements;
3. Compatibility with MRTD machine-assisted identity verification requirements;
4. Redundancy;
5. Global public perception;

---

[79] Ibid 214.

[80] Privacy International, *Background on Biometric Passports*, (30 March, 2004) Privacy International <https://www.privacyinternational.org/article/background-biometric-passports>.

6. Storage requirements; and

7. Performance.[81]

The available biometric technologies were grouped into three categories, and then assessed against these criteria.

**Table 2: Compatibility of Biometric Technologies with ICAO Criteria**

| Technology | Compatibility |
|---|---|
| Facial recognition | > 85 per cent |
| Fingerprints and irises | near 65 per cent |
| Signature, hand, and voice | < 50 per cent |

In May 2003, the ICAO's Air Transport Committee published a 'blueprint' for globally interoperable biometric passports and other travel documents. It was intended to balance expedited traveller flows with security requirements. The ICAO Technical Advisory Group on MRTDs recommended facial recognition as the globally interoperable biometric. It also suggested that this could be supplemented with fingerprint or iris recognition.[82]

Australia was active in the development of these international standards for biometric passports. Since 1995 it had been a member of the Technical Working Group responsible for assessing the feasibility and content of a technical standard. Between 2001 and 2005, the Australian Department of Foreign Affairs actively developed and tested a biometric passport.[83] Research into the use of a facial biometric identifier to connect cardinal documents of identity (birth certificates, citizenship certificates) with their owner began in 2001. The Department hoped to tie the face of a passport applicant to a name on a cardinal document. This would enable the passport information systems to scan the Department's considerable photographic

[81] Doulman and Lee, above n 2, 210–1.
[82] Ibid.
[83] Ibid 211.

database[84] and raise an alert if it detected an attempt by anyone to apply for a passport using false papers.

### *A Criticism of Biometric Passports*

The introduction of biometric passports coincided with increasing coordination of international police activities, and the practice of sending passenger data ahead of aircraft to destination airports to be compared against domestic watch lists.[85] Critics have raised concerns about these practices and technologies — particularly on privacy grounds. Privacy International and the American Civil Liberties Union argue:

> We are increasingly concerned that the biometric travel document initiative is part and parcel of a larger surveillance infrastructure for monitoring the movements of individuals globally.[86]

Other critics are concerned that biometric data, such as fingerprints and face scans, being accumulated in massive databases, could become a precursor to mass surveillance;[87] or, worse, be used by nations to monitor their citizenry unfairly and inappropriately.[88]

David Lyons, Professor of Sociology at Queens University in Canada,[89] and founder of Privacy International,[90] is concerned that 'personal data' is crossing borders at an increasingly rapid rate. He argues that borders themselves have become 'delocalised', as efforts are made to check travellers before they reach physical borders or ports of entry. He is concerned that images and information regarding travellers now circulate through different databases, looping back and forth in commercial, policing and government networks. Surveillance records, originally kept on paper in filing cabinets and

---

[84] Several million photographs of passport applicants.

[85] Doulman and Lee, above n 2, 214.

[86] Open letter from Privacy International et al to the participants of the International Civil Aviation Organization 12th session of the Facilitation Division, 30 March 2004, <https://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf>.

[87] Cath Everett, 'Biometrics-based Surveillance: Big Brother or Vital Safeguard?' (2009) 11 *Computer Fraud & Security* 5; Marie-Helen Maras, 'How to Catch a Terrorist: Is Mass Surveillance the Answer?' (2010) 5(1) *Journal of Applied Security Research* 20; Christopher S Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy' (1999) 9 *Southern California Interdisciplinary Law Journal* 295.

[88] British Broadcasting Corporation, *Concern over Biometric Passports* (30 March 2004) BBC News Technlogy <http://news.bbc.co.uk/2/hi/technology/3582461.stm>.

[89] Toronto, Ontario.

[90] An international non-government organisation.

dealing with data focused on persons in specific places, are now in digital form. They are now properly 'globalized', in the sense that they exist within patterns of global activity and social arrangements that are less constrained by geography than they used to be. Lyons contends that the 'delocalized border' is a prime example of globalised surveillance.[91]

Concerns have also been raised that biometric details could be stolen or cloned from passports.[92] Although extracting biometric data from the biometric passport would not itself enable a criminal to impersonate the holder without the holder's biometric characteristics,[93] it might be useful for other kinds of fraud.[94] If third parties were to acquire the components for making a biometric passport, cloning becomes more attractive, and (potentially) more useful.[95]

Anticipating criticism that ePassport biometric details might be misappropriated by government officials, the Australian government explicitly linked the new passport system to the *Privacy Act 1988* (Cth) to prohibit government officials from collecting, using, or disclosing personal information except in the performance of their duties.[96]

## VI A MAJOR OVERHAUL OF AUSTRALIAN PASSPORT LAW

> The package of passports legislation will provide a modern legal structure to underpin our world-class passports system.[97]

In 2005 the *Australian Passports Act 2005* (Cth) replaced the venerable *Passports Act 1938* (Cth). In his Second Reading Speech for the *Australian*

---

[91] David Lyon, above n 71, 110.

[92] Steve Boggan, '"Fakeproof" e-Passport Is Cloned in Minutes', *The Times* (online) 6 August 2008 <http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>; Tech.view, *Have Chip, Will Travel* (17 July 2009) *The Economist* <http://www.economist.com/node/14066895>.

[93] Doulman and Lee, above n 2, 214.

[94] Ibid 216.

[95] Matthew Mosk, Matthew Cole, Brian Ross and John Solomon, *Security of US Passports Called Into Question* (14 June 2010) ABC World News <http://abcnews.go.com/Blotter/security-us-passports-called-question/story?id=10909092>; Patrice Poltzer, 'Thousands of UK Passports Stolen' *Time World* (online), 28 July 2008 <http://www.time.com/time/world/article/0,8599,1827501,00.html>.

[96] *Privacy Act 1988* (Cth) ss 6 and 42–46.

[97] Commonwealth, *Parliamentary Debates*, House of Representatives, 2 December 2004, 13 (Alexander Downer, Minister for Foreign Affairs).

*Passports Bill 2004* (Cth) in the House of Representatives Main Committee, the then Shadow Minister for Foreign Affairs said:

> Fundamentally, the reason we are here today is passport security. Passport security has always been a fundamental matter of national security. In today's uncertain international environment, passport security has taken on a renewed focus. The scourge of international terrorism and the devious means by which terrorists seek to mete out their carnage on innocent civilians globally mean that we can never relent in pursuit of new technology applications to improve and tighten security around our passport system — consistent, however, with the nation's longstanding traditions of civil liberties.[98]

The Second Reading Speeches delivered by then Foreign Minister Alexander Downer and his Opposition counterpart Kevin Rudd for the *Australian Passports Bill 2004* (Cth) were remarkably similar in structure and content. Both major parties were pleased with the legislation they were about to enact. The Bill had already passed the House of Representatives back on 4 August 2004, but it had not gone further than its second reading in the Senate when parliament was prorogued for the 2004 Federal election. The Bill was reintroduced to parliament after the election, with only a few amendments. With both major parties behind it, the Bill passed uneventfully.

Mr Downer, in his Second Reading Speech, asserted that the new legislation would achieve three main objectives: to maintain the highest integrity of the Australian passport system; to ensure that passport law was complementary to national security, border security, and Australian and international law enforcement measures and cooperation; and to be consistent with Australian family law, privacy and administrative law principles.[99]

### *A Australian Passports Act 2005 (Cth)*

In 2003, the Passports Branch of DFAT had concluded, in a departmental review paper, that:

---

[98] Commonwealth, *Parliamentary Debates*, House of Representatives Main Committee, 8 December 2004, 160 (Kevin Rudd, Shadow Minister for Foreign Affairs).

[99] Commonwealth, *Parliamentary Debates*, House of Representatives, 2 December 2004, 13–14 (Alexander Downer, Minister for Foreign Affairs). This was also the view expressed by Kevin Rudd, Shadow Minister for Foreign Affairs, above n 98, 157–62, and Bruce Baird MP, Liberal Member for Cook, NSW, above n 98, 162–4, in their Second Reading speeches in support of the Bill.

> The Act, as it now stands, also does not adequately support the activities of the Passports Branch in the fight against identity fraud and misuse of Australian travel documents. Penalties imposed by the Act are not a sufficient deterrent and need to be increased to at least bring them into line with those contained in the Migration and Crimes Acts.[100]

The *Australian Passports Act 2005* (Cth) (APA 2005) came into effect on 1 July 2005. It sought to 'balance the citizen's sense of entitlement to a passport'[101] with the government's duty to protect Australia. The Act allows the government to refuse to issue passports to criminals, terrorists, persons using false identities, and to children lacking appropriate parental supervision or relevant court sanction to travel, and to cancel passports once issued. It also established the legal framework for the biometric passport.[102]

For the first time, Australian citizens — by virtue of section 7(1) of the new Act — were 'entitled, on application to the Minister, to be issued with an Australian passport by the Minister'.[103] However, the Minister needed to be satisfied as to the *identity* and *citizenship* of the applicant.[104] The Act also empowered the Department to request information from other Commonwealth and state agencies to confirm an applicant's identity.[105]

The new Act also changed the basis upon which ministerial discretion operated. It now prescribes in detail the circumstances where the Minister, or his delegate, may (or must) refuse or cancel a passport.[106] It also makes those decisions[107] reviewable under the *Administrative Appeals Tribunal Act 1975* (Cth) (AATA 1975).[108]

### *1 Security and Law Enforcement*

The Act makes it clear that '[i]f a competent authority makes a request under [section 12](1), the Minister *must not* issue an Australian passport to the person'.[109] There is no discretion to issue a passport when a '*competent*

---

[100] Australian Passports Office, above n 62.

[101] Doulman and Lee, above n 2, 216.

[102] Ibid.

[103] *Australian Passports Act 2005* (Cth) s 7(1).

[104] Ibid s 8.

[105] Ibid s 42.

[106] Ibid Division 2 of Part 2, especially ss 11–17.

[107] And other specified decisions.

[108] *Australian Passports Act 2005* (Cth) ss 48–50.

[109] Ibid s 12(2) (emphasis added).

*authority*' believes on reasonable grounds that an applicant for a passport is 'the subject of an arrest warrant issued in Australia in respect of an indictable offence against a law of the Commonwealth, a State or Territory,' or is '*prevented from travelling internationally*' by a court order, parole, or order or law of the Commonwealth.[110]

The APA 2005 defines '*competent authority*' very broadly: 'a person who has responsibility for, or powers, functions or duties in relation to, [the relevant] circumstance under a law of the Commonwealth, a State or Territory' or is 'specified in a Minister's determination as a competent authority in relation to the circumstance.'[111] To be '*prevented from travelling internationally*' includes being: '(a) required to remain in Australia; and (b) required to surrender an Australian passport; and (c) not permitted to apply for an Australian passport; and (d) not permitted to obtain an Australian passport.'[112]

It is noteworthy that the Act leaves the Minister with discretion regarding requests by a competent authority in respect of: foreign arrest warrants regarding a 'serious foreign offence'; or, restrictions on travelling imposed by a foreign court or foreign law; or, in circumstances where issuing a passport is likely to compromise foreign proceedings regarding that person's involvement or alleged involvement in a 'serious foreign offence'.[113]

The relevant 'competent authorit[ies]' include DFAT officers, Australian consular officers[114] or diplomatic staff,[115] members of the AFP, customs officers,[116] and police officers of an Australian state or territory. It also

[110] Ibid s 12(1).

[111] For example, the Minister's determination, *Australian Passports Determination 2005*, defines competent authorities for Australian law enforcement matters to be the Attorney-General (AG), the Secretary of the AGs Department, and SES employees of that department (at s 3.1) for *Australian Passports Act 2005* (Cth) s 12(3)(b).

[112] *Australian Passports Act 2005* (Cth) s 12(3).

[113] Ibid s 13(1).

[114] Within the meaning of the *Vienna Convention on Consular Relations*, opened for signature 24 April 1963, [1973] ATS 7.

[115] Within the meaning of the *Vienna Convention on Diplomatic Relations*, opened for signature 24 April 1964, [1968] ATS 3 (entered into force 25 February 1968).

[116] 'Officer of Customs' is defined by the *Customs Act 1901* (Cth) s 4(1).

includes 'an agency[117] ... that is specified in a Minister's determination as a competent authority in relation to the circumstance.'[118]

A 'serious foreign offence' is, *inter alia,* an offence with a maximum penalty of death or imprisonment for not less than 12 months;[119] or which would have been an indictable offence against the APA 2005 or another law of the Commonwealth (and specified in a Minister's determination).[120] These categories encompass most foreign offences regarding serious fraud, and terrorism, espionage, and other threats to national security.

The Minister has discretion to cancel or refuse to issue a passport where a competent authority has reasonable grounds to believe that a person is 'likely to engage in conduct ... prejudic[ial to] the security of Australia or a foreign country,' or 'might endanger the health or physical safety of other persons', or 'might interfere with the rights or freedoms[121] of other persons' or if the person's conduct might constitute an indictable offence under the APA 2005 or another law of the Commonwealth 'specified in a Minister's determination.'[122] In practice, this means offences relating to national and international security (including terrorism), illicit drugs, paedophilia or child pornography, or violent offences,[123] rather than acts which interfere with 'rights or freedoms' such as privacy.

Until the 1980s, there was strong resistance amongst Australian passport authorities to the involvement of the Passport Office in direct law enforcement. Following the Stewart Royal Commission, passport authorities have played an increasing role in detecting identity fraud and associated criminal activities, and in passing relevant information to law enforcement agencies. After 2001, this role has expanded in concert with increasing

---

[117] Within the meaning of the *Financial Management and Accountability Act 1997* (Cth). Section 5 of that Act defines an 'agency' as (a) a Department of State, including its personnel; or (b) a Department of Parliament, including its personnel; or (c) a prescribed Agency.

[118] *Australian Passports Act 2005* (Cth) s 13(3). For international law enforcement cooperation, the *Australian Passports Determination 2005* specifies, the Secretary of the AGs Department, and SES employees of that department (s 3.2(1)), or the Australian Federal Police (s3.2(2)(a)), or 'the Australian Trade Commission, to the extent that is performs consular functions within the consular district of Vancouver, Canada' (s 3.2(b)).

[119] *Australian Passports Act 2005* (Cth) s 13(3).

[120] Ibid s 14(1)(a)(v), via s 13(3).

[121] The relevant rights or freedoms being those recognised in the *International Covenant on Civil and Political Rights*, Australian Treaty Series 1980 No 23.

[122] *Australian Passports Act 2005* (Cth) s 14(1).

[123] See *Australian Passports Determination 2005*, Schedule 1.

regional cooperation[124] between passport and immigration authorities and law enforcement agencies.

The *Australian Passports Act 2005* (Cth) provides for greater cooperation between DFAT and Australasian law enforcement agencies. By 2004, Australia was exchanging passport information with countries with high traveller volumes to and from Australia. This exchange was pursued to improve the detection and prevention of the use of lost, stolen, cancelled, or otherwise invalid passports; and to facilitate travel overseas by Australians by enabling the Advance Passenger Processing scheme between partner countries. The new Act clarified the powers and responsibilities of agencies and the Minister with respect to these arrangements.[125]

> It is important, in our view, that the government continues to ensure that Australia's travel documents stay at the forefront of document security.[126]

The Opposition Foreign Affairs spokesman, Mr Rudd, was pleased to support the new legislation package as a measure that would reduce the problems flowing from lost or stolen passports.[127] However, neither he nor Mr Downer offered any specifics regarding how the new laws would achieve this goal, beyond assertions that the incorporation of emerging technologies (such as facial biometrics) would help address identity fraud.[128]

The new laws were also designed to complement other arrangements, such as those that had then recently been announced by Mr Downer at the APEC joint ministerial meeting regarding the trial of a regional 'movement alert system'. This system enables border protection officials in the USA and Australia to check passenger records and address lost or stolen passport issues.[129]

The *Australian Passports Act* was part of Australia's response to issues arising out of international security and international terrorism.[130] Both major parties agreed that the new legislation was intended to enhance security, while

---

[124] Including increased coordination and cooperation regarding efforts to counter drug trafficking, people smuggling, terrorism, and other international criminal activities.

[125] Doulman and Lee, above n 2, 218.

[126] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 2004, 157–61 (Kevin Rudd).

[127] Ibid 157–8.

[128] Commonwealth, *Parliamentary Debates*, House of Representatives, 2 December 2004, 14 (Alexander Downer, Minister for Foreign Affairs).

[129] Ibid 13.

[130] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 2004, 160 (Kevin Rudd).

maintaining community confidence that it would also adequately protect personal information.[131]

### 2 *Privacy and Security*

The key mechanism for protecting personal information under Commonwealth law is the *Privacy Act 1988* (Cth). This Act sets out a regime for the protection of '*personal information*', which is defined in section 6 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.[132]

The disclosure of personal information for the purposes of the *Australian Passports Act 2005* is addressed in Division 1 of Part 5 of the Act. Section 42 explicitly links the Act with the *Privacy Act*. It provides that, when persons are requested or directed to provide information, 'the disclosure of information by a person in response to a request or direction ... is taken to be a disclosure that is required or authorised by law'[133] for the purposes of the *Privacy Act*[134] (or similar state or territory regime).

Both major parties were satisfied that these privacy measures provide a 'transparent mechanism for obtaining information for identity and citizenship verification, and to regulate the disclosure of passport information for limited purposes'.[135] The mechanism includes arrangements for requesting information from private sector organisations.[136] However, many of the obligations placed upon disclosing organisations under the *Privacy Act* regarding obtaining the consent of, or providing notice to, individuals regarding the disclosure of their personal information to third parties are the subject of specific exemptions in the APA 2005.

---

[131] Ibid 158; Commonwealth, *Parliamentary Debates*, House of Representatives, 2 December 2004, 13-14 (Alexander Downer, Minister for Foreign Affairs).

[132] *Privacy Act 1988* (Cth) s 6.

[133] *Australian Passports Act 2005* (Cth) s 42(3).

[134] Ibid s 42(3) refers at subclause (a) to 'paragraph (1)(d) of Information Privacy Principle 11 in section 14' and at subclause (b) to 'paragraph 2.1(g) of National Privacy Principle 2 in Schedule 3 to the' *Privacy Act*.

[135] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 2004, 158 (Kevin Rudd).

[136] Commonwealth, *Parliamentary Debates*, House of Representatives, 2 December 2004, 14 (Alexander Downer, Minister for Foreign Affairs).

Parliament removed from the APA specific references to disclosure of passport information for national security purposes. It was agreed that these matters were already covered adequately in the *Privacy Act 1988* (Cth).[137] Clause 46 of the Bill (section 46 of the Act) provides a statutory regime for specified disclosures. Clause 46(d) of the Bill was removed because both the government and the opposition were satisfied that the clause would be potentially duplicative and introduce unnecessary ambiguity.[138] The *Privacy Act 1988* does not apply to the personnel or operations of the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS); these agencies report to the Inspector General of Intelligence Services (IGIS) and to the Parliamentary Joint Committee on Intelligence and Security.[139]

## VII BALANCING PRIVACY AND SECURITY

Both the Howard Liberal/National coalition government and the Labor opposition agreed that the new Act adequately balanced (individual) privacy and (community) security. However, where privacy and security interests overlap, security usually prevails. If a security, intelligence or law enforcement entity requests a disclosure, the normal practice is to disclose, often without the individual being notified or consenting.

Privacy and security are often cast as competing interests: my desire for privacy against your need for security. Security is usually regarded as the more important objective — one cannot have privacy without security, and there is no point having privacy if one is not safe enough to enjoy it.

However, privacy and security are perceptions. They are not facts. One cannot quantify how much privacy or how much security one has. One can measure how secure one feels, or assess the risks associated with securing one's environment in particular ways. This does not measure how secure one is or is not — only how probable a threat to one's security might be, in the light of specified risk factors. It is not possible to be certain about these assessments as it is not possible to have perfect knowledge of a situation.

---

[137] Ibid 14.

[138] Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 2004, 158 (Kevin Rudd).

[139] At the time of these deliberations, the committee was the Parliamentary Joint Committee on ASIO, ASIS and DSD. The name was changed on 2 December 2005.

This is not to say that it is pointless trying to assess risks — to identify as many factors as you can and estimate their probable impact and likelihood of occurring. Insurance, stock markets, public health, and public policy in general are founded upon this kind of assessment. This enables efforts to reduce or mitigate risks and their attendant consequences. Risk assessment requires the identification of events or circumstances of concern, and consideration of what could be done to reduce the likelihood of them occurring, or, if they occur, to reduce their negative impacts.[140] The development of security-enhancing and privacy-enhancing technologies is recognition of the potential for some events and behaviours to put us (or our property) at risk, and that something can, and perhaps ought, to be done to prevent them.

Technologies designed to implement and maintain security measures are important tools for implementing and maintaining privacy, but they are not sufficient. Privacy is a concern of individuals about themselves, their personal, social and emotional integrity. Security has more to do with control over physical place, space, and self. Security protects existence, but privacy is required to enjoy that existence; privacy is a concern of governments, cultures and societies, but it is experienced by individuals.

### *A Biometrics and Privacy versus Security*

The APA 2005 provides a new legal framework for the use of technology in relation to the issuing of passports. The Minister for Foreign Affairs may adopt suitable methods or technologies for identification and other purposes. Section 47 of the Act requires that a *minister's determination for use of technologies* (for example, facial biometrics) specify: (1) the nature of the information to be collected (eg a biometric — the photo provided with a passport application); and (2) the purpose for which it may be used (to assist the identification of fraudulent passport applications, and fraudulent use of passports).[141]

The Australian government chose facial recognition as the appropriate biometric tool for its passport system. Facial recognition was considered least intrusive — and easiest to comply with — as it only requires passport bearers to submit to having their photograph taken; something they were already used

[140] Standards Australia and Standards New Zealand, *AS/NZ 4360:2004 Risk Management* (2004).

[141] Commonwealth, *Parliamentary Debates*, House of Representatives, 2 December 2004, 13 (Alexander Downer, Minister for Foreign Affairs); Commonwealth, *Parliamentary Debates*, House of Representatives, 8 December 2004, 158 (Kevin Rudd).

to doing for previous passports and for other forms of (official) identification documents. This choice also enabled the Australian passport system to leverage the existing extensive collection of digitised photographs of passport applicants held by the Passport Office.[142]

Biometric technologies use statistical processes to generate a numerical value or model from a person's physical or behavioural characteristic that can be compared by a computer.[143] They are not, and cannot, be perfect. Errors leading to positive matches (false positives) or negative matches (false negatives) will occur. Even if reduced to small fractions of a percent, when applied to large populations of travellers over time, sizable numbers of persons will be inconvenienced as authorities attempt to confirm their identification. The error rate depends upon the quality of the biometric measurement captured by the system (how accurate, and precise it is),[144] and its ability to differentiate between similar enrolees (eg very similar looking people).[145]

Facial recognition systems attempt to match features in images of faces against a database of pre-recorded, known faces. The images are not directly compared. Computer software identifies as many as eighty facial features in an image and generates a mathematical model that represents the relationships between those features (distance, depth, and direction). This model is stored with other details about the person. When a face is presented to the system, a

---

[142] Some 12 million images at the introduction of the ePassport system.

[143] Anil K Jain, Arun Ross and Salil Prabhakar, 'An Introduction to Biometric Recognition' (2004) 14(1) *IEEE Transactions on Circuits and Systems for Video Technology* 4; Joseph N Pato and Lynette I Millett (eds), *Biometric Recognition: Challenges and Opportunities* (National Academic Press, 2010).

[144] Accuracy and precision are not the same thing. The accuracy of a measurement relates to how close it is to the actual (true) value being measured. Statistically, *accuracy* is the proportion of true results (both true positives and true negatives) in the total population of measurements. The fewer false positives *and* false negatives, the more accurate the measurement, and the closer any particular measurement is likely to be to the true value being measured. The *precision* of a measurement relates to how many repeated measurements (under the same conditions) will produce the exact same value. It is the proportion of true positives against all positive results — both true positives and false positives. The fewer false positives, the more precise the measurement. *Accuracy* is how close a measurement is to the true value (how close the mean of measures is to the true value), while *precision* is how close the next measurement of the same thing will be to the current measurement (the magnitude of the standard deviation of measurements from the mean).

[145] Michael E Schuckers, 'A Parametric Correlation Framework for the Statistical Evaluation and Estimation of Biometric-Based Classification Performance in a Single Environment' (2009) 4 (2) *IEEE Transactions on Information Forensics and Security* 231; 'The Difference Engine: Dubious Security', *The Economist* (online), 1 October 2010, <http://www.economist.com/blogs/babbage/2010/10/biometrics>.

mathematical model of the face is generated. It is this model that is compared against one or more already known to the system. Matches are determined based upon statistically adequate similarity between the model of the face presented and those 'matched' in the database.

The Australian passport system relies upon a comparison between the person presenting and a record stored on the passport they present at a SmartGate. This is potentially a *many-to-one* comparison: comparing the person presenting the passport with the single record on the passport requires the system to be able to distinguish the real subject from many similar looking people. The system handles failures to (adequately) achieve this match by diverting the person to manual handling.[146]

Questions have been raised about the efficacy of biometric measures as authenticators or as identifiers.[147] Biometrics may be inadequate for identifying 'known' individuals out of a large pool of unknown persons, which is required to discover a known 'person of interest' who is travelling under an assumed or stolen identity. Concerns have been raised about how adequately the quality of captured biometric data is measured, and the mechanisms by which data are compared with actual people.[148]

'Security-critical' systems, particularly those considered essential to national security, such as the passport SmartGate, are often shrouded in secrecy. This inhibits meaningful independent evaluation and verification of the design and the effectiveness of the system. The Office of the Privacy Commissioner, the Australian federal privacy agency, released an unclassified version of their 2007 Privacy Audit of the SmartGate system. While its recommendations are intact, specific details of the system that were considered sensitive for law enforcement and security reasons were withheld at the request of Customs.[149]

---

[146] Australian Customs and Border Protection Service, *How It Works* (2009) <http://www.customs.gov.au/site/page5831.asp> ; Australian Customs and Border Protection Service, *SmartGate — Frequently asked questions* (2010) <http://www.customs.gov.au/site/page5555.asp>.

[147] Joseph N Pato and Lynette I Millett (eds), *Biometric Recognition: Challenges and Opportunities* (National Acadamies Press, 2010); Jay Stanley and Barry Steinhardt, *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida* (2002) American Civil Liberities Union <http://www.biometrie-online.net/images/stories/dossiers/technique/visage/drawing_blank.pdf>; 'The Difference Engine', above n 145.

[148] Roger Clarke, *Biometrics' Inadequacies and Threats, and the Need for Regulation* (2002) Xamax Consultancy <http://www.rogerclarke.com/DV/BiomThreats.html>; Pato and Millett, above n 146.

[149] Office of the Privacy Commissioner, SmartGate Automated Border Processing: Final Audit Report (2007).

In his review of biometric systems, Roger Clarke argues that they must not be used unless and until a comprehensive and strictly enforced regulatory scheme is in place. This scheme must require openness of their design and implementation, with independent testing and verification of published results and privacy impact assessments *before* field tests or deployment of production systems take place, and a commitment to privacy-sensitive/privacy-aware system architectures.[150]

False positives can result in people being treated as if they were criminals 'just in case'. But a match by the system is not proof that the person matched is indeed the person of interest, nor does a failure to match prove otherwise. Computers can only indicate that two sets of data are similar enough, or dissimilar enough, according to criteria programmed into them.

It is crucial to recognise, therefore, that biometrics do not and cannot address the *quality* of the information in any record that may be associated with the biometric. Biometrics cannot ensure that the record with which they are associated contains accurate, or current, information regarding the person from whom the biometric is derived.

Privacy law is largely concerned with identification and identity data. We refer to this as 'information privacy'. It prescribes limits on the acquisition and use of information that can be used to identify individuals.[151] This can put it at odds with security and law enforcement agencies which increasingly demand more and better identification and surveillance of individuals. Governments have to manage these competing interests, but it may be more fruitful to look for synergies between privacy and security. Understanding the limits of identification and the means available to identify individuals provides a sound foundation upon which to (re)consider the balance made between privacy and security in these critical information infrastructure and national security systems.

## VIII CONCLUSION

Over the past thirty years, the balance between privacy and security in Australia's passport system has shifted from concern for the privacy of individuals towards broader national security interests. This has been

[150] Clarke, above n 148.

[151] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Final Report No 108 (2008).

cemented in the last decade by an emphasis on anti-terrorism measures that are reflected in security policies.

Governments around the world are looking to establish 'gold standard' identity credentials as part of their national security (anti-terrorism) strategies. As part of this effort, they are looking to biometric technologies to enable conclusive association between a 'secure' credential and a single individual. Biometric technologies establish a statistical profile of certain physical characteristics which are matched against those of persons presenting themselves to a system in order to either confirm or deny a match. These and other new technologies are being deployed to improve security by identifying fraudulent documents and potentially dangerous 'persons of interest'.

At the same time, the efficacy and social impacts of these technologies are being questioned. The technical capacity of systems to evade exploitation or to distinguish reliably friend from foe creates an 'arms race' between securers and exploiters, and has the potential to promote a culture of fear. This is compounded by concerns regarding the effects of these technologies upon the nature and foundations of social and personal identity, and the relationships associated with them. In the rush to nail down everyone's 'identity', or to capture the value of it, there is a possibility that the very purpose of having an identity will be trampled. Privacy may all too easily be displaced in the rush to protect security.

Privacy is a complex social value. It is not immutable. Thus it is overly simplistic to assume that security is always more important. Privacy and security often relate to the same social problems, where they interact in important ways. They can appear to have different purposes because they offer different perspectives on the same concerns. Rather than 'balancing' privacy against security, it is more fruitful to consider how they interact, and where they might reinforce one another. Context is important, and privacy and security are both concerned with relationships — and it is within relationships that identities (and information regarding them) have meaning.