PRIVACY ISSUES FORUM

WELLINGTON, NEW ZEALAND 28 MARCH 2003

25 YEARS OF EVOLVING INFORMATION PRIVACY LAW - WHERE HAVE WE COME FROM AND WHERE ARE WE GOING

The Hon Justice Michael Kirby AC CMG[*]

---

[*] Justice of the High Court of Australia. One-time Chairman of the Australian Law Reform Commission; Chairman of the OECD Expert Group on Transborder Data Flows and the Protection of Privacy and of the OECD Expert Group on Data Security.

IN THE BEGINNING

There are three reasons that have inveigled me out of the citadel in Canberra where I perform my duties as a Justice of the High Court of Australia, involved only rarely now in issues of privacy[1].

The first is that I never miss an opportunity to cross the Tasman to lay claim to Australasia's lost two States. It is difficult for an Australian to understand why New Zealanders have so far proved obdurately impervious to the blandishments of federation. Membership by New Zealand of the Australian Commonwealth is envisaged by the preamble to the Australian Constitution Act[2]. Yet so far, New Zealand has stubbornly declined our invitations. It has done so despite my own generous (if unauthorised) offer of two States, special protections for the Maori and huge subsidies for a joint enterprise to win the America's Cup back for Australasia.

In the context of privacy I would just mention one of the advantages of federation so that it can hang in the air during this forum.

---

1 An exception is *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

2 *Commonwealth of Australia Constitution Act* 1901 (UK) 63 & 64 Vict Ch 12, preamble.

A federal system of government offers a form of planned inefficiency. It divides great power. At a time in history when technology is vastly increasing the efficiency of privacy invasions, a system of government that superimposes divisions of lawmaking and governmental power may have found new and previously unnoticed advantages.

Secondly, I come across the waters to pay tribute to Bruce Slane, foundation Privacy Commissioner of New Zealand. He completes his eleven years as Commissioner on 12 April 2003. His retirement from the office is a watershed in the development of privacy law and practice in New Zealand, indeed in this part of the world. The forum also marks the tenth anniversary of the *Privacy Act* 1993 (NZ). Some of the more interesting recent features of privacy law and practice in New Zealand have attracted vigorous comment[3]. Over all of the developments that have ushered in the implementation of the national privacy laws of New Zealand, Bruce Slane has presided.

From the outset, he had to address many urgent and sensitive problems. No sooner than he arrived in office, but he was caught up in the *Pugmire* case concerning disclosures made by a Wanganui Hospital psychiatric nurse, acting as a "whistle-blower"[4]. The problems have not

---

[3] B Roth, "Recent Developments in New Zealand Privacy Law" (2002) 9 *Privacy Law and Policy Reporter* 121; New Zealand, Law Commission (Preliminary Paper 49), *Protecting Personal Information from Disclosure* (2002).

[4] *Consumer* (June 1997), 360.

become easier for Commissioner Slane and his colleagues since then. On the contrary, they have become more numerous, more urgent, more technical and more difficult.

I first knew Bruce Slane when I was a young judge inaugurating the Australian Law Reform Commission. I came to New Zealand for a law conference in Auckland in the emid-1970s. Mr Slane was already a leading member of the New Zealand Law Society. We hit up a friendship that has endured nearly three decades. I discovered in him a kindred interest in the communication of legal issues through the media to the legal profession and to the general community that it serves. We were both fascinated by the way the media operates. We saw in its operation both potential for enhancing public policy debates and risks, including risks of unreasonable invasion of individual privacy. The potential and the risks have each grown during the period of our friendship. But we both know how important modern media is to human freedom.

I pay tribute to Bruce Slane for his devoted work for privacy in New Zealand and in the world. I praise his outreach to ordinary citizens that has been a hallmark of his activity and a reason for his success. I hope that his techniques will be continued by his successor[5].

---

[5] A tribute to Bruce Slane in implementing the New Zealand Act and conducting the first review of it after three years of operation can be found in T McBride, "The Review Process - Taking on the Critics" (1998) 5 *Privacy Law and Policy Reporter* 101.

The third reason for my presence is that it affords me the opportunity to reflect on twenty-five years of the *Guidelines on Privacy* of the Organisation for Economic Cooperation and Development (OECD). The work of the Expert Group of the OECD that drafted the *Guidelines* began in Paris in 1978. At the first meeting I was elected to chair that Group. That event proved a pivotal point in my own career. Not only did it involve me closely with a group of brilliant antagonists in the development of the basic principles of information privacy that have gone on to influence the law in Australia[6], New Zealand[7] and beyond. It also exposed my mind to a rude awakening to an aspect of law which, up to that time, had largely been neglected in my legal eduction. At first hand I saw the way in which international law was made. True, the "law" on this occasion was the "soft law" of the OECD *Guidelines on Privacy Protection*[8]. But the lesson was not lost on me. In a very short time, I discovered how:

- Global technology was forcing the pace of international legal and policy developments[9];

---

6 *Privacy Act* 1988 (Cth).

7 *Privacy Act* 1993 (NZ). The Act became fully operational in July 1996.

8 OECD, *Guidelines on the Protection of Privacy and Transborder Data Flows* (Paris, 1981).

9 M D Kirby, "Access to Information and Privacy: The Ten Information Commandments" 55 *Cincinatti Law Review* 745 at 750-751 (1987).

- Such developments had very large economic, cultural and legal implications;
- Despite the divergences caused by these factors, the necessity of finding common ground (or more accurately of avoiding radically different approaches to a common technology) provided an enormous stimulus to the development of international norms; and
- The work of international bodies could actually be of practical help to domestic law-makers. Confronted by new, controversial, technological and potentially divisive problems, local rule-makers naturally looked to trusted international agencies and their expert bodies to give a lead that would provide a foundation for uniform, or at least compatible, national laws on topics of international concern.

An appreciation of the importance of globalisation and regionalisation for the law is an eye-opening idea. So far, it has proved elusive to most lawyers. Most are content to live in the calm backwaters of their own jurisdiction. Yet in the age of jumbo jets, of cyberspace, of the human genome, of space travel and global problems like AIDS and terrorism, municipal jurisdiction is increasingly coming under the challenge of global and regional developments. Amongst the emerging norms are the statements of universal fundamental human rights. Amongst the fundamental human rights is that established by Article 17 of the *International Covenant on Civil and Political Rights*, guaranteeing the right to privacy. Universal fundamental human rights is one of the most powerful ideas at work in the law today throughout the world. It is

not yet dominant; but the dangers of the alternatives will surely make it so.

Many lawyers, whose minds are still locked in the pages of their law school written down taken before 1978 when the OECD Group first gathered, may be dubious about these propositions. But, having seen the way international law is changing and impacting domestic jurisdiction, I am an evangelist for the truth. It beckons us to a new and different legal era, suitable to a new millennium where lawyers must find common ground and shared principles with colleagues in other countries. Privacy protection is such a topic.

The Privacy Commissioners of Australia, New Zealand and the region know this to be true. Indeed, the Privacy Commissioners of the world meet regularly to track the developments of technology, law, business and practice and to share experience and ideas. It is good that they do for nowadays, truly, privacy and data security are global topics. The technology laughs at paltry efforts to make them purely local.

PRIVACY IN THE COURTS

After I rejoined the mainstream of the law in appellate courts after my decade in the Australian Law Reform Commission, I was struck by the utility of the OECD *Guidelines* when issues of general principle concerning the flow of information came up for consideration. But I have also been struck by the fact (noted in the Australian Law Reform

Commission Report on *Privacy* [10]) that the common law sometimes has difficulty in formulating general principles or effective remedies for privacy protection. This was especially surprising given the importance that the English, from whom the common law derived, normally paid to individual privacy as a value to be respected in society.

Last year a case came before the High Court of Australia in which submissions were made to the Court to repair the omissions of the law and to invent a common law right to privacy which would be upheld in Australia to protect a corporation that claimed that its privacy had been invaded. The case involved many interesting legal questions. It arose out of the action of an unidentified party planting a hidden camera in private premises from which was procured film, later partly telecast, showing the circumstances in which native animals were slaughtered for export as food.

I will not detail all the legal complications that arose. Some of them concerned the federal Constitution and the implied right to free expression in Australia that has been discovered as an implication from the system of representative democracy established by the constitutional text. Interestingly enough, the latest word on that implication was written in a case brought to the High Court by David Lange, one-time Prime Minister of New Zealand[11]. His affection for Australia was so strong that

---

[10] Australian Law Reform Commission, *Privacy* (ALRC 22) 1983.

[11] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

he was determined to leave a lasting mark on Australia's constitutional law; and he did. But if I go into that aspect of the case I may only discourage such enthusiasts as still exist in New Zealand for the federal idea; so I will desist.

For present purposes, the interest of the *Lenah Game Meats*[12] case is two-fold. First, it signalled a growing interest of some of the High Court judges (including myself) to reopen consideration of the general development of civil remedies for privacy invasion which, in Australia, was largely stillborn after a possibly erroneous misreading of the decision of the High Court in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*[13], decided in 1937.

The *Game Meats* case was not a particularly good vehicle to allow a definitive re-exploration of the general idea of privacy protection. In so far as this would, in turn, be stimulated by the contents of Art 17 of the ICCPR, that provision appears to relate only to privacy of the human individual. It does not seem apt to apply to a corporation or agency of government. Nevertheless, noticing a number of recent developments in United States law[14], where the Supreme Court has discerned a "strong

---

[12] cf *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

[13] (1937) 58 CLR 479.

[14] eg *Cox Broadcasting Corporation v Cohn* 420 US 469 at 488-489 (1975).

tide running in favour of the so-called right of privacy" and developments in New Zealand law[15], Canadian law[16] and English law[17], it now seems far from certain that an Australian protection of privacy under the common law might not be developed in a suitable case involving an established invasion of the privacy of a human person.

The other importance of the recent decision of the High Court of Australia, as noted by David Lindsay in an article that heroically endeavoured to chart the various streams of opinion in the decision, was the disparity over fundamentals disclosed in the reasons of the participating judges. Mr Lindsay remarked somewhat sharply[18]:

> "Taking these considerations into account, it is suggested that the relatively ad hoc, somewhat chaotic reasoning of the High Court in the *Lenah* decision is an example of what can happen in a legal system that refuses to take individual rights seriously and that, as a result, has an inadequate legal framework for recognising and protecting individual rights. While judicial recognition of an Australian tort of privacy would improve the position of individuals under the general law, an adequate legal regime must await the extra-judicial development of a Bill of Rights. As this seems unlikely, it

---

15 Tobin, "Invasion of Privacy" [2000] NZLJ 216; *P v D* [2000] 2 NZLR 590 at 599-601. See also *Lenah Game Meats* (2001) 208 CLR 199 [325].

16 A Linden, *Canadian Torts Law* (6th ed, 1997), 56; *Aubry v Duclo* (1996) 141 DLR (4th) 683.

17 *R v Broadcasting Standards Commission; Ex parte BBC* [2001] 3 WLR 1327; cf *Lenah Game Meats* (2001) 208 CLR 199 [326].

18 D Lindsay, "Protection of Privacy Under the General Law Following *ABC v Lenah Game Meats Pty Ltd:* Where to Now?" (2002) 9 *Privacy Law and Policy Reporter* 102 at 107.

> would seem that protection of rights and freedoms under Australian law is destined to be influenced indirectly by developments elsewhere. By this, I am referring mainly to European human rights jurisprudence, via its effect on substantive principles of English law, including confidentiality law. In this sense, the relatively unsatisfactory reasoning evident in the judgments in *Lenah* is symptomatic of fundamental weaknesses in the structure of Australian law, just as much as it is a reflection of fundamental differences of opinion among the members of the current High Court".

The United Kingdom courts, which in the past have been such an important source for the common law in courts in Australia, New Zealand, Hong Kong and elsewhere in the region, are now (as Mr Lindsay's comment notes) directly under the influence of the European Convention. Perhaps this is so by way of the *Human Rights Act* 1998 (UK). This is why, in several recent cases[19], the English courts have lately proved much more receptive to arguments seeking judicial protection for the privacy of individuals than was formerly the case[20].

Those who look to the courts as a new and revived source of privacy law in common law countries, after a long sleep lasting most of the last century, can therefore probably take heart from the recent trend of judicial authority. It would not be the first time that the courts had developed the common law in a kind of symbiosis with developments of statute law. In my view, a similar process has occurred in respect of the common law principle governing the right to reasons for administrative

---

19 eg *Douglas v Hello! Ltd* [2001] 2 WLR 992.

20 A point noted by Gummow and Hayne JJ in *Lenah Game Meats* (2001) 208 CLR 199 [112]-[116].

decisions at a time when so many statutes have been enacted, by legislatures everywhere, to spell out that right in recognition of contemporary social values that demand its fulfilment[21]. So the only advice that I can offer on this interesting development on privacy protection in the courts is: watch this space.

INSTITUTIONAL DEVELOPMENTS

In the twenty-five years since the OECD Expert Group on Privacy met under the chandeliers of the Château de la Muette in Paris, there have been enormous changes in the world, and in the technology of information distribution and processing. So great have been these changes that, in May 1999, *The Economist*[22] proclaimed on its cover: "The End of Privacy". It described, in vivid detail, the features of "the surveillance society" that had led it to this gloomy diagnosis.

Nothing that has happened in the four years since that declaration has reduced the problem which that distinguished journal called to notice. On the contrary, the Internet has continued to expand rapidly,

---

[21] cf *Osmond v Public Service Board* [1984] 3 NSWLR 447 at 465. But see *Public Service Board (NSW) v Osmond* (1985) 159 CLR 656 at 669-670 and see now *Baker v Minister of Citizenship and Immigration* [1999] 2 SCR 815; *Mukherjee v Union of India* [1990] Supp 1 SCR 94.

[22] 1 May 1999, 11, 17-19.

the use of the World-Wide-Web doubling every twelve months[23]. William Gibson's vision of cyberspace comes ever closer[24].

The particular difficulties of reconciling this new zone of human knowledge and activity was well illustrated by yet another recent decision of the High Court of Australia involving a defamation claim brought in Victoria for a news story uploaded on the Web in New York or New Jersey in the United States[25]. The case vividly illustrated once again the difficulty, glimpsed as through a glass darkly by the OECD Group twenty-five years ago, of stamping national legal regimes upon transborder flows of data.

Three and a half years ago, at the twenty-first international conference on privacy and personal data protection in Hong Kong, I examined the extent to which the 1980 OECD *Guidelines* remained relevant and useful in these new technological circumstances and the extent to which they were showing signs of their age[26].

---

[23] R Miller, "The Internet in Twenty Years: Cyberspace the New Frontier" (OECD, Paris, 1997); cf M D Kirby, "Privacy in Cyberspace" (1998) 21 *UNSW Law Journal* 323; L A Bygrave, *Data Protection Law* (Klewer, 2002) 29; E Longworth, "The Possibilities for a Legal Framework for Cyberspace - Including a New Zealand Perspective" in UNESCO, *The International Dimensions of Cyberspace Law,* Vol 1, (Ashgate, 2000), 9.

[24] W Gibson, *Neuromancer* cited in E Frank, "Can Data protection Survive in Cyberspace?" (1997) 8(2) *Computes and Law*, 20.

[25] *Dow Jones and Co Inc v Gutnick* (2002) 77 ALJR 255.

[26] M D Kirby, "Privacy Protection - A new Beginning" (2000) 18*Prometheus* 125 and in papers of Hong Kong, Office of the

Footnote continues

One of the greatest challenges to the effectiveness of the *Guidelines* has been the provision of extensive indexes on Internet sites such as *Yahoo* and the *Altavista* search engine. The *Guidelines* of 1980 were prepared on the context of the technology then known. That was before webcrawlers, spiders, robots and trawlers were introduced that could subject personal data to fresh surveillance against criteria different from those for which the data had originally been collected and possibly unknown or even non-existent at the time of such collection.

It was these changes that led me to a number of suggestions for new privacy principles relevant to contemporary technology. I listed them in late 1999. All of them remain relevant today[27]:

- A right in some circumstances not to be indexed;
- A right in some cases to encrypt personal information effectively[28];
- A right to fair treatment in key public infrastructures so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy;

Privacy Commissioner for Personal Data, *Privacy and Personal Data, Information Technology and Global Business in the Next Millennium* (1999), 2.

[27] cf Victorian Law Reform Commission, *Defining Privacy* (2002).

[28] OECD, *Guidelines for Cryptography Policy* (Paris, 1997), 27 (OECD Doc C (1997) 62/Final). cf J Adams, "Encryption: The Next Best Thing?" (1998) 2 *Computers and Law* 39 at 40.

- A right, where claimed, to human checking of adverse automated decisions and a right to understand such decisions affecting oneself[29]; and
- A right, going beyond the aspirational language of the "openness principle" in the OECD *Guidelines,* of disclosure of the collections to which others will have access and which might affect the projection of the profile of the individual concerned[30].

The growth of e-commerce has led to concern amongst computer users and Net users both about privacy and security of personal data, a point noted by Stephen Lau of Hong Kong[31]. The right of users to be informed in advance of the provider's policy on data privacy and to have a choice of anonymity for browsing and transacting business, encryption and collection and use of sensitive data is also a subject of expressed concern. The provider may have current strategies and policies that are communicated to the user. Yet these are always subject to supervening obligations imposed on the provider by law for the purpose of enforcement of new criminal offences (eg access to prohibited

---

29 G Greenleaf, "Privacy Principles - Irrelevant to Cyberspace?" (1996) 3 *Privacy Law and Policy Reporter* 6 at 114, 118.

30 R Clarke, "Profiling and Its Privacy Implications" (1994) 1 *Privacy Law and Policy Reporter* 7 at 128-129; R Wacks, "Privacy in Cyberspace: Personal Information, Free Speech and the Internet" in P Birks (ed) *Privacy and Loyalty* (Oxford, 1997) 93.

31 S Lau, "E-Commerce, Consumer Rights and Data Privacy" [3rd Quarter, 19098] *I-Ways*, 37 at 38; cf L Gamertsfelder & Ors, *E-Security* (Lawbook Co, 2002).

pornographic Websites), intellectual property protection and revenue protection.

In addition to these considerations, the advance of the Human Genome Project to its effective completion, ahead of schedule, in 2003 coincides with yet another important anniversary - the fiftieth commemoration of the discovery by Watson and Crick on 28 February 1953 of the elements of DNA.

The potential use of DNA and modern systems of genetic data to provide a vast range of sensitive health data about the individual, as well as a secure and virtually unique means of identifying the individual, presents large and puzzling questions for privacy protection in the future. Such questions will occupy privacy commissioners, law reform agencies, policy makers and legislators in the years ahead.

Amongst the questions that are raised by the use of DNA in this connection are those concerning:

- Non-consensual DNA testing;
- Consensual DNA testing for research;
- Use of discarded DNA for purposes of health, employment, insurance and criminal record checks;
- Collection of data based on DNA material that profoundly affects the life choices of the individuals concerned; and

- Invasion of genetic data banks and unauthorised dissemination or publication of genetic data about the individual[32].

Little wonder that actual and potential misuse of genetic information has already occurred. The Australian Law Reform Commission has signalled its continuing involvement at the cutting edge of these issues. In August 2002 it published a Discussion Paper of nearly a thousand pages dealing with a vast range of questions concerned with access to genetic testing; the use of information and health data; the need for anti-discrimination law; the requirement for enforcing the *Australian National Statement on Ethical Conduct in Research Involving Humans*; the encouragement of best practice in human genetic research; special rules for human tissue collection, the ownership of human genetic samples, the establishment of genetic registers; the provision of genetic counselling and medical education; the conduct of genetic screening; the use of genetic data for discrimination in insurance and employment; the availability of DNA parentage testing; the use of DNA in immigration decisions, forensic procedures, criminal investigation, post-conviction activity and civil proceedings. This is an indication of the enormous variety of questions that will need to be tackled[33]. The ALRC report on these topics has now been provided to

---

[32] R Curley and L Caperna, "The Brave New World is Here - Privacy Issues and the Human Genome Project" (2003) 70 *Defense Counsel Journal* 22-35.

[33] Australian Law Reform Commission, *Protection of Human Genetic Information* (2002) (DP 66). The International Bioethics Committee of UNESCO is preparing an *International Declaration on Human*

Footnote continues

the Federal Attorney-General. It must be tabled in the Australian Parliament by mid-June 2003.

TERRORISM AND PRIVACY

At the time of this Forum, the thoughts of most informed people go out to the military and civilian personnel engaged by the conflict in Iraq. That conflict has grown out of the extraordinary events of 11 September 2001 when many features of our world changed[34]. In consequence of such changes, laws have been enacted or proposed in many countries, including Australia. Such laws and the practices that have gathered around them, have been designed to enhance the capacity of society to respond to the perceived dangers of terrorism and breaches of national security and the criminal law. Enhancement of the power of police and national security agencies in many lands has obvious implications for the legal protection of individual privacy. In a time of war or of terrorism, there is a tendency if not for the law to fall silent at least for its defence of basic civic freedoms to become somewhat muted.

Genetic Data which is expected to be placed before the General Conference of UNESCO in October 2003. This elaborates the UNESCO *Universal Declaration on the Human Genome and Human Rights* (1997).

[34] G Williams, "One Year On - Australia's Legal Response to September 11" (2002) 27 *Alternative Law Journal* 212 referring to Security Legislation Amendment (Terrorism) Bill 2002 (Cth).

From the point of view of privacy regulators, the issues arising from anti-terrorism laws are highly relevant to the purposes for which they have been established. However, they tend to remain on the fringes of the jurisdiction of privacy agencies given the wide exemptions commonly found in their powers so far as they touch national security and intelligence activities. Such exemptions have not, however, prevented privacy guardians from raising concerns about perceived over-reach of security laws.

Some have done this in private, knowing that, in the current sensitive climate, their views on such subjects, if expressed in public, are likely to be marginalised or ignored. On the other hand, some Privacy Commissioners, whom Lord Denning would doubtless have described as "bold spirits", have felt entitled or even obliged to make public comments on this topic. Thus the Canadian Privacy Commissioner, Mr George Radwanski, recently challenged the Canadian Government on several issues arising out of this concern. By doing so, he raised the profile of the debate on the inter-relationship of privacy protection and security protection in Canada.

In the Canadian Commissioner's overview to the Privacy Commissioner of Canada's *Annual Report* to Parliament, released in January 2003, Mr Radwanski remarked[35]:

---

[35] Canada, Privacy Commissioner, *Annual Report* to Parliament 2001-2002, Commissioner's Overview.

> "It is my duty … to report a solemn and urgent warning to every Member of Parliament and Senator and indeed to every Canadian. The fundamental human right to privacy in Canada is under assault as never before. Unless the Government of Canada is quickly persuaded from its present course of parliamentary action and public insistence, we are on a path that may well need to the permanent loss not only of privacy rights that we take for granted but also of important elements of freedom as we now know it. We face this risk because of the implications, both individual and cumulative, of a series of initiatives that the Government has mounted or is effectively moving forward. These initiatives are set against the backdrop of September 11, and anti-terrorism is their purported rationale".

Specifically, the Canadian Commissioner questioned the creation of new "Big Brother" passenger data bases for international transport; the dramatic enhancement of state power to monitor communications; a suggested introduction of a national ID card with biometric identifiers; and the support for video-surveillance of public streets by the RCMP[36].

The Commissioner's report is blunt speaking and critical of proposed legislation for a *Public Safety Act*, changes to the *Criminal Code* and the introduction of practices to step up the surveillance of persons in and out of Canada. He acknowledges the dangers that terrorists present to freedom and civic values, including privacy. But he urges that Canadian society remain faithful to the tolerant values that terrorism seeks to attack. Otherwise, he points out, the terrorists will have succeeded in their basic attack on our freedoms.

---

36 *Ibid*, 2.

I make no comments on these remarks. They are certainly deserving of close attention[37]. In most countries, including my own, legislation is under active consideration to enhance official powers having unmistakable implications for individual human privacy.

In the same spirit as the Canadian Commissioner, the American Civil Liberties Union in January 2003 issued a report warning of the growth of the surveillance society in the United States. The report *Bigger Monster Weaker Chains*[38] is relatively brief. It provides a useful synthesis of developments in video surveillance, data surveillance, genetic privacy, biometrics, communications technology, government data bases and the extension of the power of government agencies. The thesis of the ACLU report is that "we are being confronted with fundamental choices about the sort of society we want to live in"[39].

Interestingly, the ACLU report draws to notice a recent decision of the Supreme Court of the United States in *Kyllo v The United States*,

---

[37] M D Kirby, "Australian Law - After 11 September 2001" (2001) 21 *Australian Bar Review* 253, contrasting the decisions of the High Court of Australia in *Australian Communist Party v The Commonwealth* (1951) 83 CLR 1 and the Supreme Court of the United States in *Korematsu v United States* 323 US 214 (1944) and *Dennis v United States* 341 US 494 (1950).

[38] American Civil Liberties Union, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*.

[39] *Ibid*, 15.

decided after 11 September 2001. There the Court held that a reasonable expectation of privacy could not be determined by the power of new technologies. In a decision written for the Court by Justice Antonin Scalia, the Supreme Court held that without a warrant, the police could not use a new thermal imaging device that searches for heat sources to conduct what was the functional equivalent of a warrentless search for marijuana cultivation in Mr Kyllo's home. Specifically, the Court declined to leave the privacy of that home "at the mercy of advances in technology"[40].

GETTING & KEEPING THE BALANCE

Obviously, getting the balance between the protection of society and the protection of individual privacy has never been easy. In the age of civic danger and terrorism, keeping our heads and preserving the proper equilibrium will surely be one of the great challenges for privacy agencies in the years ahead. So much seems to conspire against the defence of individual privacy. But this fact merely makes it all the more important that we defend and uphold this cherished human right and precious feature of our society.

For his sterling work in pursuing and attaining these goals, I applaud Bruce Slane and I honour his achievements and those of his

---

[40] *Kyllo v United States* 190 F 3d 1041 (2001).

colleagues in New Zealand. They set a fine example to the region and the world. Now new participants must pick up the responsibilities that others carried earlier. In Isaac Newton's words, we stand on the shoulders of those who went before. Here in New Zealand they were broad and strong shoulders. The challenges that lie ahead will be new and unpredictable. Who would have imagined forty years ago where we now stand.

PRIVACY ISSUES FORUM

WELLINGTON, NEW ZEALAND 28 MARCH 2003

25 YEARS OF EVOLVING INFORMATION PRIVACY LAW - WHERE HAVE WE COME FROM AND WHERE ARE WE GOING

The Hon Justice Michael Kirby AC CMG