Prometheus, Vol. 21, No. 4, December 2003

Twenty-five Years of Evolving Information Privacy Law—Where Have We Come From and Where Are We Going?[1]

MICHAEL KIRBY

ABSTRACT *The author chaired two Expert Groups of the OECD including that on privacy, whose guidelines form the basis of the legal regimes in Australia, New Zealand and many other countries. He reviews the success of those guidelines and the defects disclosed by time and by the remarkable advances in information technology since the guidelines were adopted in 1980. He then explores the revival of interest in the protection of privacy in the courts as a common law entitlement, instancing the recent decision of the Australian High Court in the* Lenah Game Meats Case. *The difficulty which the common law faces in responding to the challenge of informatics is then explored by reference to the decision in* Dow Jones v Gutnik *concerned with liability for defamation on the Internet. Finally, the author considers two contemporary problems: genetic privacy and terrorism. On the latter, he concludes with a reminder of the need to uphold civic rights, including privacy, so as to ensure that the terrorists, although losing, do not win.*

Keywords: privacy, relevance of advances in technology, Australian acceptance of a tort of privacy, genetic data privacy and its protection, terrorism and privacy, protection of basic human rights whilst combating terrorism.

In the Beginning

A forum on privacy issues in March 2003 affords me an opportunity to reflect on 25 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 the group. That event proved a pivotal point in my professional career. Not only did it involve me closely with a collection of brilliant antagonists in the development of the basic principles of information privacy that have since influenced the law in Australia,[2] New Zealand,[3] and beyond, it also exposed me to a rude awakening about an aspect of law which, up to that time, had largely been neglected in my legal experience. At first hand, I saw the way in which international law and policy were made. True, the 'law' on this occasion was the 'soft law' of the

Prometheus ISSN 0810-9028 print/ISSN 1470-1030 online © 2003 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/0810902032000144664

OECD *Guidelines on Privacy Protection*,[4] 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;[5]
- such developments had very large economic, cultural, legal and safety implications;[6]
- despite the divergences caused by the causative factors, the necessity of finding common ground (or more accurately of avoiding radically different approaches to a common technology) provided a significant 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 jurisdictions. 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* (ICCPR), guaranteeing the right to privacy. Throughout the world universal fundamental human rights is one of the most powerful ideas at work in the law today. It is not yet dominant; but the dangers of the alternatives will surely soon make it so.

Many lawyers, whose minds are still locked in the pages of their law school lecture notes, written down before 1978 when the OECD Group on Privacy first gathered, may be sceptical about these propositions. But, having seen the way international law is changing and impacting upon domestic jurisdiction, I am an evangelist for the truth. It beckons us to a new and different legal era, suitable to a millennium in which lawyers and other specialists must find common ground and shared principles with colleagues in other countries. Privacy protection is one such 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 so. Nowadays, truly, privacy and data security are global topics. The technology laughs at paltry efforts to make them amendable to purely local laws.

Privacy in the Courts

After I rejoined the mainstream of the practice of law in appellate courts in Australia, following 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*[7]) 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.

In 2001 a case came before the High Court of Australia in which submissions were made asking it to repair the omissions of the law and to invent a common law right to privacy to be upheld in Australia.[8] The issue arose in a case that involved a claim to protect a corporation that asserted that, unless restrained, its privacy had been invaded, and would continue to be, by a media organisation. The case involved many interesting legal questions. It grew 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 of the legal complications that arose in the case. Some of them concerned the Australian Constitution and the implied "right to free expression" 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 has been written in a case brought to the High Court by the Rt Hon David Lange, one-time Prime Minister of New Zealand.[9] His affection for Australia was so strong that he was determined to leave a lasting mark on Australia's constitutional law; and he did.

For present purposes, the interest of the *Lenah Game Meats* case is two-fold. First, it signalled a growing interest on the part of some of the High Court judges (including myself) to reopen consideration of the general development of civil remedies for privacy invasion that, in Australia, was largely stillborn after a (possibly erroneous) reading of the decision of the earlier High Court in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*,[10] decided in 1937. The *Game Meats* case was not a particularly good vehicle to encourage a definitive re-exploration of the general idea of privacy protection. In so far as this would be stimulated by the provisions of Art. 17 of the ICCPR, that provision appears to relate only to privacy of the human individual. It does not seem apt to be applied to a corporation or agency of government. Nevertheless, noticing a number of recent developments in United States law,[11] where the Supreme Court has discerned a 'strong tide running in favour of the so-called right of privacy' and developments in New Zealand law,[12] Canadian law,[13] and English law,[14] it now seems possible that an Australian protection of privacy under the common law might be developed in a suitable case involving an established invasion of the privacy of a human being.

The second importance of the recent decision of the *Game Meats* case, as noted by David Lindsay in an article that heroically attempted to analyse the various streams of opinion in that decision, was the disparity over fundamentals disclosed in the reasons of the several participating judges. Mr Lindsay remarked, somewhat sharply:

> 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 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.[15]

The United Kingdom courts, which in the past have been such an important source of the common law for 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 on Human Rights*. This is now the case, directly, because of the *Human Rights Act* 1998 (UK). That is why, in several recent decisions,[16] the English courts have proved much more receptive to arguments about judicial protection for the privacy of individuals than was formerly the case.[17]

Those who look to the courts as a 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 have developed the common law in a kind of symbiosis with developments of statute law.[18] In my view, a similar process has occurred in respect of the common law principle governing the right to reasons for administrative decisions at a time when so many statutes have been enacted, by legislatures in many countries, to spell out that right in recognition of contemporary social values that demand its fulfilment.[19] 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 25 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 these changes been that, in May 1999, *The Economist*[20] 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 newspaper called to notice. On the contrary, the Internet has continued to expand rapidly, the use of the World Wide Web more than doubling every 12 months.[21] William Gibson's vision of cyberspace comes ever closer.[22]

The particular difficulties of reconciling this new zone of human knowledge and activity were 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.[23] The case vividly illustrates, once again, the difficulty, glimpsed as through a glass darkly by

the OECD group 25 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.[24] 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 environment of the technology then known. That was before webcrawlers, spiders, robots and trawlers were invented that, in the context of the Internet, 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:[25]

- a right in some circumstances not to be indexed;
- a right in some cases to encrypt personal information effectively;[26]
- 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 his or her privacy;
- a right, where claimed, to human checking of adverse automated decisions and a right to understand such decisions affecting oneself;[27] 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.[28]

The growth of e-commerce has led to concern amongst computer and Internet users both about privacy and security of personal data, a point noted by Stephen Lau of Hong Kong.[29] 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 indeed communicated to the user. Yet these are always subject to supervening obligations imposed by law on the provider for the purpose of enforcement of new criminal offences (e.g. access to prohibited 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 contemporary 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.[30]

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.

The foregoing list provides an indication of the variety of questions that will need to be tackled.[31] The ALRC report on these topics was provided to the Federal Attorney-General in April 2003. It was released in late May 2003 following its tabling in the Australian Parliament.[32]

Terrorism and Privacy

During 2003 it has been impossible to ignore the implications for the protection of privacy and other civil liberties of the global response to acts of terrorism and the dangers of the misuse of weapons of mass destruction. Early in the year the world watched, with concern and mixed feelings, the conflict in Iraq. That conflict was a direct result of the extraordinary events in the United States of 11 September 2001 when many accepted features of the world changed.[33]

As a 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 societies to respond to the perceived dangers of terrorism and breaches of national security and of the criminal law. Enhancement of the power of police and of national security agencies 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 confined.

From the point of view of privacy regulators, the issues arising from such 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 exemptions typically found in their legislative powers so far as they touch national security and intelligence activities. Such exemptions have not, however, prevented some privacy guardians from raising their concerns about the over-reach of security laws.

Some have done so 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 then Canadian Privacy Commissioner, Mr George Radwanski, challenged the Canadian Government on several issues arising out of this concern. By doing so, he raised the profile of the debate in Canada on the inter-relationship of privacy protection and security protection.

In the Commissioner's overview published with the Privacy Commissioner of Canada's *Annual Report* to Parliament, released in January 2003, Mr Radwanski remarked:

> 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 lead 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.[34]

Specifically, the Canadian Commissioner questioned the creation of new 'Big Brother' passenger databases for international transport movements; the dramatic enhancement of official powers to monitor individuals' communications; a suggested introduction of a national ID card containing biometric identifiers; and support for video-surveillance of public streets by the Royal Canadian Mounted Police.[35]

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

These remarks are clearly deserving of attention.[36] 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 (ACLU), in January 2003, issued a report warning of the growth of the surveillance society in the United States. That report *Bigger Monster, Weaker Chains*[37] is relatively brief. It provides a useful synthesis of developments in video surveillance, data surveillance, genetic privacy, biometrics, communications technology, government databases 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'.[38]

The ACLU report draws to notice a recent decision of the Supreme Court of the United States in *Kyllo v The United States*,[39] 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 warrantless 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] There will be more such cases of this kind before the courts. In many countries, such as Australia and New Zealand, there are no constitutional protections equivalent to those successfully invoked in the United States.

Getting the Balance

Obviously, getting the balance between the protection of the claims and interests of society and the protection of individual privacy has never been easy. In an 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 before us. 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 that belongs to every individual in accordance with international human rights law.

Notes and References

1. Adapted from an address to the Privacy Issues Forum, Parliament House, Wellington, New Zealand, 28 March 2003.
2. *Privacy Act* 1988 (Cth).
3. *Privacy Act* 1993 (NZ). The Act became fully operational in July 1996.
4. OECD, *Guidelines on the Protection of Privacy and Transborder Data Flows*, OECD, Paris, 1981.
5. M. D. Kirby, 'Access to information and privacy: the ten information commandments', *Cincinatti Law Review*, 55, 1987, pp. 750–1.
6. M. Rees, 'The final countdown', *New Scientist*, 3 May 2003, p. 33.
7. Australian Law Reform Commission, *Privacy* (ALRC 22), 1983.
8. *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.
9. *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
10. *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.
11. See for example, *Cox Broadcasting Corporation v Cohn* 420 US 469 at 488–9 (1975).
12. See for example, *P v D* (2000) 2 NZLR 590 at 599–601; F. Tobin, 'Invasion of privacy', *New Zealand Law Journal*, 2000, 216. See also *Lenah Game Meats* (2001) 208 CLR 199 [325] and New Zealand Law Commission, *Protecting Personal Information from Disclosure*, Preliminary Paper 49, 2002.
13. A. Linden, *Canadian Torts Law*, 6th edition, 1997, p. 56; *Aubry v Duclo* (1996) 141 DLR (4th) 683.
14. *R v Broadcasting Standards Commission; Ex parte BBC* [2001] 3 WLR 1327; cf *Lenah Game Meats* (2001) 208 CLR 199 [326].
15. D. Lindsay, 'Protection of privacy under the general law following *ABC v Lenah Game Meats Pty Ltd:* where to now?', *Privacy Law and Policy Reporter*, 9, 2002, pp. 102, 107.
16. For example, *Douglas v Hello! Ltd* [2001] 2 WLR 992.

17. A point noted by Gummow and Hayne JJ in *Lenah Game Meats* (2001) 208 CLR 199 [112]–[116].
18. *Cotogno v Lamb [No 3]* (1986) 5 NSWLR 559 at 570–2; but see *Lamb v Cotogno* (1987) 164 CLR 1 at 11.
19. See *Osmond v Public Service Board* (1984) 3 NSWLR 447 at 465, but see *Public Service Board (NSW) v Osmond* (1985) 159 CLR 656 at 669–70 and see now *Baker v Minister of Citizenship and Immigration* [1999] 2 SCR 815; *Mukherjee v Union of India* [1990] Supp 1 SCR 94.
20. *The Economist*, 1 May 1999, pp. 17–9. See also C. Varney, 'The death of privacy?', *Newsweek Special Edition*, December 2000–February 2001, pp. 78–9.
21. R. Miller, *The Internet in Twenty Years: Cyberspace the New Frontier*, OECD, Paris, 1997; cf. M. D. Kirby, 'Privacy in cyberspace', *UNSW Law Journal*, 21, 1998, p. 323; L. A. Bygrave, *Data Protection Law*, Kluwer, Amsterdam, 2002, p. 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, London, 2000, p. 9.
22. W. Gibson, *Neuromancer*, cited in E. Frank, 'Can data protection survive in cyberspace?', *Computes and Law*, 8, 2, 1997, p. 20.
23. *Dow Jones and Co Inc v Gutnick* (2002) 77 ALJR 255.
24. M. D. Kirby, 'Privacy protection—a new beginning', *Prometheus*, 18, 2, 2000, pp. 125–32, and in papers of Hong Kong, Office of the Privacy Commissioner for Personal Data, *Privacy and Personal Data, Information Technology and Global Business in the Next Millennium,* 1999, p. 2.
25. See Victorian Law Reform Commission, *Defining Privacy*, 2002.
26. OECD, *Guidelines for Cryptography Policy*, [OECD Doc C (1997) 62/Final], Paris, 1997, p. 27; compare with J. Adams, 'Encryption: the next best thing?', *Computers and Law*, 2, 1998, p. 39.
27. G. Greenleaf, 'Privacy principles—irrelevant to cyberspace?', *Privacy Law and Policy Reporter*, 3, 1996, pp. 114, 118.
28. R Clarke, 'Profiling and its privacy implications', *Privacy Law and Policy Reporter*, 1, 1994, pp. 128–9; R. Wacks, 'Privacy in cyberspace: personal information, free speech and the Internet', in P. Birks (ed.), *Privacy and Loyalty*, Oxford, 1997, p. 93.
29. S. Lau, 'E-commerce, consumer rights and data privacy', *I-Ways,* 37, 3rd quarter, 1998, p. 38; compare with L. Gamertsfelder and Ors, *E-Security*, Law Book Co, 2002.
30. R. Curley and L. Caperna, 'The brave new world is here—privacy issues and the Human Genome Project', *Defense Counsel Journal*, 70, 2003, pp. 22–35.
31. 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 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.
32. Australian Law Reform Commission, *Essentially Yours—The Protection of Human Genetic Information in Australia*, ALRC 96, 2003.
33. G. Williams, 'One year on—Australia's legal response to September 11', *Alternative Law Journal*, 27, 2002, p. 212, referring to Security Legislation Amendment (Terrorism) Bill 2002 (Cth).
34. Canada, Privacy Commissioner, *Annual Report* to Parliament 2001–2002, Commissioner's Overview.
35. *Ibid*, p. 2.
36. M. D. Kirby, 'Australian law—after 11 September 2001', *Australian Bar Review,* 21, 2001, p. 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).
37. American Civil Liberties Union, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, 2003.
38. *Ibid*, p. 15.
39. *Kyllo v The United States* 533 US 27 (2001).
40. *Ibid.*