COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Reference: Law enforcement implications of new technology

MONDAY, 26 MARCH 2001

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **http://www.aph.gov.au/hansard**

To search the parliamentary database, go to: **http://search.aph.gov.au**

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Monday, 26 March 2001

Members: Mr Nugent *(Chair)*, Senators George Campbell *(Deputy Chair)*, Denman, Ferris, Greig and McGauran and Mr Edwards, Mr Hardgrave, Mr Kerr and Mr Schultz

Senators and members in attendance: Senators Denman and George Campbell and Mr Hardgrave, Mr Kerr, Mr Nugent and Mr Schultz

Terms of reference for the inquiry:

The Committee will inquire into the law enforcement implications of new technology, with particular reference to:

a. whether use of new technology by law enforcement agencies is adequately catered for by Commonwealth, State and Territory legislation;

b. the extent to which electronic commerce facilitates the laundering of the proceeds of crime; and

c. whether international law enforcement cooperation is adequate to meet the challenges of new technology.

WITNESSES

Committee met at 9.33 a.m.

SALIER, Ms Mary-Jane, General Counsel, UUNET and OzEmail Internet; and Representative, Internet Industry Association

CHAIR—I declare open this fourth public hearing of the parliamentary Joint Committee on the National Crime Authority inquiring into the law enforcement implications of new technology. I welcome our first witness today, Ms Mary-Jane Salier, who is general counsel to UUNET and OzEmail Internet. She is appearing today on behalf of the Internet Industry Association. I am advised that you have actually stepped into the breach on the IIA's behalf at relatively short notice, so we are most appreciative of you making yourself available today. I understand that in the absence of the IIA not being able to prepare a formal submission, it is your intention to provide the committee with copies of a number of IIA papers relevant to our terms of reference from which we will be able to glean the association's views. Is that correct?

Ms Salier—Yes. If not today, I will be providing papers in the future. I have some papers today, but unfortunately the website was down on Friday when I was getting the papers together.

CHAIR—We will accept those at a later date, that is fine. The committee prefers that all evidence be given in public, but you may at any time request that your evidence, part of your evidence or answers to specific questions be given in camera, and the committee will consider any such request. I believe you plan to make an opening statement before we move to questions. So I invite you to make your opening statement.

Ms Salier—Thank you. At the outset, let me say that the Internet Industry Association is very grateful for the opportunity given to it by the parliamentary committee to address key issues and concerns relating to the Internet service provider industry—which I will now refer to as the ISP industry—which have arisen out of the committee's investigations into the law enforcement implications of new technology.

Firstly, I would just like to say a little bit about the Internet Industry Association, which I will refer to from now on as the IIA. The IIA is Australia's national Internet industry organisation and was established in 1995. Members include telecommunications carriers, content creators and publishers, web developers, hardware vendors, banks, Internet law firms, ISPs, Internet research analysts and a range of other businesses providing technical and professional support services to the industry. The IIA currently has over 300 corporate and business members. The IIA has a number of functions, including the provision of policy input to government and advocacy of a range of business and regulatory issues, as well as the promotion laws and initiatives that enhance access, equity, reliability and growth of the medium within Australia.

It should be made perfectly clear to the committee that the IIA's objectives are all about promoting and facilitating the growth, technical development and efficient functioning of the Internet in Australia as an open system, raising consumer and small business confidence in using the Internet, particularly for the purposes of e-commerce and initiating the supporting programs to promote that goal. Most importantly, our objective is to promote laws which facilitate unrestricted and open use of the Internet, and the use of the Internet, by as many Australians as possible.

The IIA has a strong track record in promoting end user welfare, having pioneered codes of practice for online content regulation in Australia. These codes are achieving international recognition for their innovative approach to protecting end user welfare in a way that does not impede the growth and development of the industry. The association also has a strong track record in working with regulators—for example, the Racing and Gaming Administration in New South Wales, where it has struck a cooperative accord underpinned by ministerial regulation to help ensure ISP cooperation in the enforcement of New South Wales gambling legislation.

In addition, the IIA is represented on a number of high level governmental committees, including the Australian Information Advisory Council; NetAlert, which is the Internet content community advisory body; and the Critical Information Infrastructure consultative group, formerly the NII or the National Information Infrastructure group, which deals with issues of national security. The IIA has also embraced the need for protection of personal information on the Internet and is developing a code of practice for registration with the Privacy Commissioner later this year. This work is designed to set minimum benchmark standards for industry to ensure that end user confidence in using the Internet, particularly for e-commerce, is maximised. For a full list of committees on which the IIA is represented, we refer the committee to the IIA website, which is www.iia.net.au/contact.html.

The industry itself, according to the Australian Bureau of Statistics, and as at the end of September 2000, was comprised of 718 ISPs supplying Internet access services across Australia, with a small number of large ISPs providing the majority of services. The eight largest ISPs—and by large I mean that they have more than 100,000 subscribers—provided Internet access to 2.3 million or 60 per cent of all Internet subscribers. The ABS statistics also show there were 3.8 million Internet subscribers registered in Australia at the end of the September quarter 2000, downloading more than one billion megabytes of data over the previous three months. Of these subscribers, 400,000 were registered as business or government subscribers, and these accounted for 43 per cent of the total data downloaded.

The issues being discussed here today affect a substantial portion of the population of Australia, not to mention the direct effect on the ISPs that, as noted, comprise over 700 small to large businesses on the Australian landscape. The reason I raise this is to highlight where the impact lies with certain suggestions made by other witnesses and submitting organisations to this committee. The IIA did not make a written submission into the subject matter of the hearing today. However, it is with grave concern that we have read the submissions made by other parties and the transcripts of the proceedings to date. I think it is of benefit to outline the range of issues of particular concern to our industry raised by previous submissions and transcripts.

The submission of the Australian Securities and Investments Commission, ASIC, included extensive references to what they think ISPs should be obligated to do. ASIC called for various areas to be addressed. At page 48 of volume 1 of the submissions, ASIC expressed their concern that there was no present general law to require ISPs to retain records. ASIC suggested that the Proceeds of Crime Act 1987 was a good model for retention to be applied—that is, there were certain specified records that the industry would have to retain for a certain period of time, with penalties applying in the event of failure to comply.

At page 49 of volume 1 of the submissions, they suggested that there should be some compulsion for monitoring by ISPs of their subscriber's activities. Again, the Proceeds of Crime Act

1987 was cited as a model in this area. Under division 3 of part 4 of that act, an order may be applied to direct a financial institution to monitor all transactions conducted through a certain account of one of its customers. Again at page 49, there was a suggestion that agencies should be empowered to require the removal of illegal Internet material and serve notices to stop ISPs providing services to customers. The notices to stop providing services in this case were for people that were found to be in contravention of the Corporations Law.

The Minister for Police in Western Australia also spent part of his submission, which was at page 109 of volume 1, discussing the obligations of ISPs. In that submission, it was stated that the ISP's obligations under section 282 of the Telecommunications Act were reliant upon the cooperation of ISPs, and these obligations were easy to circumvent and manipulate. The minister said:

> Consequently an ISP that chooses to be uncooperative, for criminal or other motives, has a number of options available to thwart the efforts of law enforcement agencies attempting to obtain information.

This general call then drilled down to specifics, as the submission goes on to call for effective legislation to require ISPs to be cooperative and to retain records. The last point of the submission, in so far as it related to the ISP industry, was that it was the minister's opinion that regulation by codes of conduct is insufficient to guard against criminal activities in light of growth of the Internet and Internet based crime.

The issue was also briefly mentioned by the Australian Bureau of Criminal Intelligence, whose submission is found at page 121 of volume 2. In that submission, several interim findings are set out as a result of the bureau's current investigations into the child pornography area. One of the findings is that, whilst most ISPs are cooperative with law enforcement agencies, consideration should be given to all ISPs having to maintain records. It is also interesting to note that it is recognised by the bureau that most larger ISPs already retain adequate records.

The last submission that raised issues specific to our industry was that of the National Crime Authority at page 142 of volume 2. Like the WA police, the NCA noted that law enforcement agencies cannot be assured of ISP assistance in all cases and that a low level of regulation raises the risk of compromising investigations. The NCA believes that regulation equals accountability for ISPs and this would lead to improved cooperation from ISPs. The submission notes that a component of the regulations should be to require ISPs to receive identity documents from their customers in order to satisfy themselves as to the identity of their subscribers.

Obviously a plethora of issues have been raised for the industry by these submissions including, in relation to privacy, technology capability, costs, enforcement and so on. A common theme through all of the submissions relates to the retention of records. It is interesting to note that at no stage do any of the submissions attempt to define exactly what the records are that they are requiring the ISPs to maintain. If you look at the submissions and transcripts, the term 'records' is referred to in a wide variety of ways. For example, ASIC refers to records as 'the details of communications that have taken place and the parties to the communications'. At the same page, ASIC also refer to log records of proxy servers as being records for the purposes of their discussion. The WA police refer to records as being specific logs and other information relating to the use of ISP systems that may be required to identify those involved in criminal

activities. At page 5 of the 6 November transcripts, Mr Marshall Irwin, a member of the NCA, says:

> What is important is that the ISPs keep their records for a sufficient period of time to enable law enforcement to gain access to them, just as it gains access to call charge records from the carriers under the telecommunications act to indicate who has been talking to whom at what time, so that similar information is available in relation to those people who are using the Internet to communicate.

This point is crucial to the proceedings and how the industry will respond. Is it as simple as access records that these issues are directed at? For example, OzEmail, the ISP that I work for, does in fact record and retain logs noting when its customers log in and log out of its service by reference to the unique user identification that each of its customers has. This information is collected for legitimate billing purposes. Many other ISPs would also record this information, but it is important to note that not all do. If this is the information that is sought to be retained, then there are different issues than if it is seriously being suggested that we should retain information relating to every customer that logs in and what that customer does with whom online, what sites they visit, what transactions they conduct, what news groups they frequent and what chat sessions they participate in. The salient point here is that, unlike call charge records, we are not dealing with point to point communications.

Depending on how that word 'records' is defined results in a dramatic difference in impact on industry, privacy and community. For example, if we take the broad use of the word as given by the ASIC, it is akin to asking a carrier to record every telephone conversation made over its system or asking Australia Post to photocopy every letter that passes through its office. This is not an overdramatic analogy. An ISP does not have an interest in recording or monitoring what its customers do once access is gained to the Internet, except for the purposes of providing its service obviously. ISPs do not track or monitor customer activities or communications. ISPs do not record and maintain such information. There are very good reasons for this.

Firstly, there is simply no value in this information for Internet access providers. Secondly and most importantly, there are privacy considerations and implications raised by this conduct. These are enormous, as you can imagine, and a critical issue to an ISP's business as it is a longstanding phenomenon that privacy issues are consistently found to be a real barrier to use of the Internet. Our growth is dependent upon finding a way to assure the users that their privacy will be not only respected but also vigorously guarded.

Thirdly, there are the costs and technical considerations. The size of the systems needed to track and monitor every customer who uses our systems would be enormous. This would again be dwarfed by the size of the database that would be needed to store this information. The idea of records being defined in this way and required to be logged and maintained cannot seriously be entertained. We present two examples to demonstrate the impact of such requirements on ISPs—one with 500,000 subscribers and one with one million subscribers. We have assumed that the average storage space for each customer's activity logs, which is every HTTP request made, would be approximately 78 kilobytes a day. This is an assumption based on our knowledge of the average customer's activities and we believe it is conservative in nature. In the first case of 500,000 subscribers the database would grow 39 gigabytes a day and at the end of one year would be approximately 14,235 gigabytes in size. In the second case it would obviously be double these figures—that is, it would grow at 78 gigabytes a day and at the end of one year would be well over 28,000 gigabytes in size.

We have just done a rough calculation—this is by no means accurate—to ascertain the cost of storage of this data for 12 months in a retrievable format. The cost in respect of the lower figure would be in excess of $3 million for the hardware alone. The calculation was based on using Sun A5200 arrays as the hardware and includes processing power and tape backups. There is little allowance made for any spare processing capabilities in these figures. Supporting a doubled user base could double that cost or, more likely, could mean taking some of the storage to near-line or off-line with tape robots, special software, et cetera. This would also cover your backups. That type of system is called a hierarchal storage array system—HSA system—which might save up to 50 per cent of the storage cost taken off-line, but obviously slows access to non-real-time in the event you would want to retrieve off-line or near-line data. So a HSA system for one million users would probably cost in the order of $4.5 million, instead of $6 million for a totally online system.

Racking, power, administration and the like would be around $200,000 per annum. There would also be some application and/or software development costs. This could range from tens of thousands to hundreds of thousands, depending on the sophistication of the query tools required. In any event, you can see that the costs are substantial and in the current economic climate would be the final straw for many ISPs.

To come back to privacy, I again emphasise the significant concerns of telecommunications users and, indeed, ISPs about privacy. ISPs, as noted before, have to overcome concerns in the community in order for their businesses to survive, but, more importantly, ISPs also have serious consequences to face if they are found to be in breach of privacy obligations imposed upon them by section 276 of the Telecommunications Act. These issues need to be balanced against the legitimate interests of law enforcement agencies.

On 4 February 2001, an interesting article appeared in the *Age* which highlighted the privacy concerns in the community. The article was entitled ‘Anger at Plundered Phone Records’ and it was by the *Age*’s political correspondent, Brendan Nicholson. It concerned the reaction to recently released figures from the Australian Communications Authority which confirmed that telecommunications companies passed information to law enforcement and other government agencies almost one million times in the 1999-2000 period. The reaction, of course, was one of privacy outrage by privacy groups and certain politicians.

We think that privacy issues must continue to be delicately balanced. Records need to be sensibly defined, and access to those records must be adequately controlled. If this is achieved then the issues become those of enforcement of such collection, and I will address the enforcement issue shortly.

A number of other issues are raised in the submissions. The only one that I will specifically address is ASIC’s suggestion that ISPs should be made to monitor customer activities in certain instances. We would submit that ASIC is de facto suggesting an extension of the interception of communication regime currently governed by the Telecommunications (Interception) Act. This act has also been the subject of discussion within the submissions and the proceedings of this committee. The focus has been on the need for balance and accountability when distributing such powers. Needless to say, the IIA is fully supportive of the concept of the need for balance and accountability for agencies when seeking to use such powers. Interception of communications is a drastic power to bestow, as it necessarily involves a complete invasion of

privacy. Powers such as these should only be available on a last resort basis and under stringent guidelines. In fact, the IIA vigorously opposes any extension of such powers beyond the act in which they currently lie.

This brings us back to the problem of how to deal with issues raised by law enforcement agencies so that agencies and industries are cooperating and are satisfied with what is being asked for and what is being received. The first point to note here is the rhetoric which is often applied in respect of this industry—the recognition of the need to have a light touch, co-regulatory legal environment in order to balance the competing interests of fostering the Internet environment and satisfying the security and regulatory needs of our nation. This concept is, in fact, enshrined in section 4 of the Telecommunications Act, where it is noted that telecommunications need to be regulated in a manner that promotes the greatest practicable use of industry self-regulation and does not impose undue financial and administrative burdens on participants in the industry.

This month, the Australasian Centre for Policing Research released a paper entitled 'Electronic Crime Strategy of the Police Commissions' Conference Electronic Crime Steering Committee 2001-2003'. In that paper, a number of guiding principles were expounded at page 5, including:

> Private sector leadership and self regulation wherever possible, and practical regulation where necessary, complemented by effective and mutually beneficial partnerships with police ...

The paper also has a view expounded on regulation and legislation, as this is one of its strategy focus areas. The view is expressed at page 18 of that paper:

> There is also a recognition of a need for 'light touch' regulation and consideration of broader economic and social imperatives. Jurisdiction is complicated by the global reach of electronic crime and police seek flexibility in the law to allow for extra territorial prosecution of offenders, and where possible, harmonisation of laws. Further, police recognise they are one of several government agencies with responsibilities to investigate electronic crime, and seek law making that does not create unenforceable laws or place unrealistic expectations on enforcement capabilities.

The IIA endorses this approach and, as noted, has a good track record in relation to the co-regulatory environment.

There is no doubt that investigations such as the commission's are happening all around the world. The IIA itself is in the process of gathering information from our European and American colleagues in order to try and ascertain exactly what approaches are being taken to those issues in other countries. The IIA's view is that the way forward is not by precipitous legislation developed as a reaction to new types of crime being committed, or the fact that traditional crimes are being carried out in a new medium. Rather, the way forward is to ascertain the world's best practice and apply it in the Australian landscape in a cooperative manner.

The IIA proposes the following. Firstly, the IIA will continue to work with the law enforcement agencies to develop a protocol for dealings between ISPs and law enforcement agencies. Our proposal is that this protocol should be developed after examining best practice in other countries around the world. It should also be developed in a spirit of cooperation between the law enforcement agencies and the ISPs so as to ensure maximum effect and benefit. Secondly, the IIA will encourage its members to abide by this protocol as it has done successfully in the

past. The IIA has an excellent track record at providing education and assistance to its members as well as to other industries in order to achieve desired outcomes in respect of issues such as these. On this point, the IIA is also happy to offer to provide education and training to the law enforcement agencies in respect of the Internet industry.

At this point it is pertinent to raise what the IIA perceives as being an enormous issue for the industry and law enforcement today—namely, the shortage of skills and resources within the law enforcement agencies in Australia to deal with cybercrime. In the transcripts of the proceedings dated 2 March 2001, it was noted by Mr Kerr, a committee member:

> Coming back to law enforcement and retaining people with competence, the number of people in the law enforcement environment in Australia with skills in these areas seems to me to be quite small. I understand roughly, ballpark figures, the AFP has 12 people for the whole of Australia who are cybercrime experts.

This does not come as any surprise to us in the industry, because in our day to day dealings with law enforcement officers it is clear there is a lack of fundamental understanding of the industry, of the technology and even of the information that they are requesting in the pursuit of their investigations. Although the IIA understands that the focus of this committee is on the NCA and organised crime, it believes that we cannot sensibly have a discussion on law enforcement and technology without focusing on both ends of the scale.

As noted by Ms Sandra Ellims from the Attorney-General's Department, who appeared as a witness on 4 December 2000:

> The range of e-crime activity potentially includes intellectual property theft, denial of service attacks, child pornography, fraud, virus propagation, spamming, the dissemination of offensive materials, commercial espionage, sabotage, electronic terrorism, cyber stalking, extortion, tax evasion and money laundering and I am sure that that is not an exclusive list.

A myriad of issues arises relating to the lack of resources being allocated by—or perhaps allocated to—the various law enforcement agencies around Australia. This is not to say that there are not pockets of individuals within the various agencies who are very savvy in respect of this kind of crime, but the fact is that there are just not currently enough resources to deal at an adequate level with cybercrime. We speak from experience here as the industry has to deal with agencies at all levels—from ASIO to the Federal Police down to the local boys in blue. It is also our experience—and again it is not surprising—that what limited resources are available to the law enforcement agencies are allocated in areas of specific interest to those agencies rather than in response to requests made by ISPs.

The IIA has recently set up the Law Enforcement Taskforce, which is chaired by IIA Director and OzEmail Chief Executive Officer, Justin Milne, in an attempt to identify these and other issues, work with the law enforcement agencies towards satisfactory resolution and set out a strategy whereby the IIA can assist its members in understanding and assisting the law enforcement agencies while ensuring that privacy concerns of our customers are addressed and no unfair burdens are placed on the industry.

In closing I will briefly mention the draft convention on cybercrime currently being negotiated. The treaty has been drafted by representatives of the 41 nation Council of Europe and the United States, Canada, Japan and South Africa, all of whom hold observer status with the Council of Europe. The proposed draft is the first international treaty to address criminal law

and procedures for dealing with offending behaviour directed at computer systems, networks or data and other similar abuses. The draft convention covers the destruction of data or hardware, as well as the distribution of child pornography, theft of copyright and intellectual property, and other crimes that could be carried out over the Internet.

Additionally, it provides law enforcement authorities with the basis to investigate 'any crime for which there is evidence that might be stored on computers'. The document defines 'offences' and addresses questions on liability of individual and corporate offenders and the minimum standards for the applicable penalties. The treaty was referred to by Mr Karl Alderson, who is also from the Attorney-General's Department, at page 49 of the 4 December 2000 transcript. Mr Alderson said:

> The cybercrime convention, being developed by the Council of Europe with involvement of a number of other countries, in particular the United States, is a document that draws on expertise and experience from a whole range of countries and is there as a model that all participating countries and others can draw on in terms of offences and enforcement powers.

The IIA counsels caution in this approach, as this treaty is the subject of some vigorous objections from the ISP industry in both Europe and America. Issues with the treaty include corporate liability, service provider liability, immunity when providing assistance to law enforcement and service provider obligations. The provisions on corporate liability include criminal liability for corporate officers and establish new legal standards for the online world that differ from the offline world. In relation to service provider liability, the treaty should, but does not explicitly, exempt service providers from liability if illegal activity is conducted or illegal content is stored or transmitted by means of their network. In relation to immunity when providing assistance to law enforcement, the treaty should, but does not, provide complete immunity to ISPs for any claims or damages arising from an entity's acts carried out in good faith reliance upon a law enforcement order or demand.

In relation to service provider obligations, the same debate which has been raised here in relation to retention of records is being carried on in relation to that treaty as well, as the convention imposes various requirements on service providers to preserve, intercept and disclose data to law enforcement for unspecified periods of time. In general, the treaty is excessively broad and vague in its terms, opening it up to inconsistent interpretation. I apologise for the length of this opening statement, however, due to our lack of submission I believe there were a number of issues that we needed to canvass before I took questions from the committee.

CHAIR—Thank you for that. There is a lot there in short order, but we will try to come to grips with it.

Ms Salier—I am actually happy to provide a copy of the opening statement to the committee, if you would like.

CHAIR—We also have it on *Hansard*.

Ms Salier—Right. I actually have a copy of the papers that I mentioned.

CHAIR—That would be useful. Could you give those to the secretary?

Ms Salier—Yes.

CHAIR—I do not think you mentioned in your statement the legislation in the UK—the UK Regulation of Investigatory Powers Act 2000—which, as I understand it, requires ISPs to maintain their capability for inception and decoding. Does your association have a view on that legislation?

Ms Salier—Our view would be that the legislation itself, we think, was not properly thought out before being introduced. The reason I made no substantive comment on it is that the legislation was introduced and then a lot was left to further debate, being defined by codes of practice and so on. The government still has to set down the regulations for exactly what the intercept capability and the like is going to be defined as. Obviously the industry in the UK is trying to work as best it can with the legislation as it has been brought down, and get it down to a level that the industry feels it can reasonably work with.

There is an interesting paper—and I do not know if you have had the benefit of viewing it—which was done by the British Chambers of Commerce with help from the London School of Economics in respect of the regime. The report summarised the specific areas of commercial and economic activity which were likely to be adversely affected by RIP, as it currently stands, which included direct costs to ISPs of implementing, maintaining and running interception equipment and support; recurrent cost of equipment designed to meet changing RIP requirements; costs associated with securing legal and professional advice and additional insurance costs; displacement of investment in new operations to non-UK jurisdictions in that they think, especially in relation to the encryption access powers, that a lot of companies will be moved to host their systems offshore, rather than under the reach of the RIP act; loss of confidence and trust amongst e-commerce consumers; a loss of UK share in the global e-commerce market; the cost of management; and the revocation of revoked keys. Obviously once a key has been handed over to an enforcement agency, the act allows you to revoke them, and that would be the most sensible course to take once they have been disclosed.

Analysis under this report concludes that the compliance costs to ISPs alone are likely to be in the order of £640 million in the first five years of RIP's operation. The report goes on to predict that, overall, financial implication of RIP in terms of both losses and leakages from the UK economy, and of the cost of implementation, may well be in the order of £46 billion in the first five years of operation. The government, however, commissioned the Smith report on the cost, which the government still stands by, which placed only a $30 million price tag on intercepting communications on the Internet.

Mr KERR—One of the dilemmas here, I suppose, is that we are grappling with new areas which experience cannot have taught us lessons about. You speak of best practice and I guess your idea of best practice is likely to be very different from law enforcement's best practice, and they would point to Britain as a model and ISP providers would point to some other environment where your costs are less.

In terms of costs and your strategies to deal with those issues, you would appreciate the social costs of things like tax avoidance, money laundering and the like, diminish in terms of multiples—those sorts of numbers that you are talking about. How do we draw the line? You are talking about the balances and suggesting least impact responses. I would prefer us to try to

look at what we are actually seeking to be able to examine through law enforcement and to decide what we are willing to allow law enforcement to have access to and what we are not willing to allow it access to, and then work back to a least cost solution for that. Have you any ideas about the areas of communication which you believe law enforcement should have access to, given that a large amount of communication and business is now being conducted in this environment?

Ms Salier—Without an interception warrant, I believe that law enforcement should not have access to any content of communications. That is one line that the IIA would definitely draw in the sand. In relation to other records that law enforcement providers may have access to, currently under section 282 of the Telecommunications Act they can request information or records that are stored by ISPs which mainly includes information that can be gained from a request such as for on-line time spent by the community, by users, as opposed to the content of the communication that is occurring during the time that they are on line.

I strongly believe that privacy considerations dictate that there should be no general storage of the content of communication and that there should be no general access to the content of communications without the appropriate checks and balances such as those that are currently laid out under the Telecommunications (Interception) Act. Whilst we appreciate the concerns that law enforcement agencies are trying to address and deal with, the fact is that the privacy implications are enormous with the Internet, much more so than, for example, the carriers intercepting telephone conversations. The Internet is not a point-to-point medium and if we go back to the national privacy principles, the first principle is in relation to collection, namely, the collection of data should not be intrusive. I think that anything above and beyond records that you need for your billing purposes or recording when users log on and log off the Internet is intrusive and therefore needs to be subject to greater scrutiny.

Mr KERR—You say at the moment that the Telecommunications (Interception) Act is the bottom line. How would that operate with respect to a suspicion, for example, that somebody is engaged in money laundering, tax evasion or using encrypted email to negotiate a drug deal?

Ms Salier—Under the Telecommunications (Interception) Act, once the agency involved has satisfied all of the requirements of that act in relation to the issue of a warrant, it is served upon the carrier, the ISP or whichever is the body involved with whom the suspected offender is a customer, and then the requirement is dependent on what is set out in the warrant in relation to the interception of email and passing it to the agency that has issued the warrant.

Mr KERR—What about encryption issues?

Ms Salier—Encryption issues are difficult, but currently the legislation does not require us to de-encrypt communications that are sent over our network. The encryption is an end-user issue. Obviously, we may encrypt some of the communications that are passing through our network, but essentially with the communications that you are referring to, encryption is placed by the end-user, not by the ISP. Therefore, requiring—

Mr KERR—You may or may not have keys for that, is that correct?

Ms Salier—We would not have the keys to it.

Mr KERR—You may or may not.

Ms Salier—We may or may not, but more likely than not we would not have the keys to de-encrypt. The agency would be just as likely to have keys to de-encrypt or resources to de-encrypt those communications. Essentially, it is because we have no interest in de-encrypting communications, as opposed to agencies which do.

Mr KERR—In Britain, what is the issue with encryption? There is an obligation to provide—

Ms Salier—Encryption keys.

Mr KERR—But on whom does that obligation fall?

Ms Salier—On whoever holds the key. I have not gone chapter and verse into the RIP act, but I think the obligation largely would fall upon people who host other people's company servers and therefore may provide some form of encryption in relation to those company servers, otherwise it would fall upon companies themselves who encrypt their communications that are providing e-commerce services or perhaps just encrypt in the normal course of business.

Mr KERR—Would you have any objections to an obligation to provide such keys?

Ms Salier—Absolutely.

Mr KERR—In those circumstances?

Ms Salier—In most circumstances, yes—in all circumstances, because, firstly—

Mr KERR—But that does not affect your business.

Ms Salier—It does affect our business, because it causes a loss of consumer confidence in using the Internet when—

Mr KERR—It imposes no cost on your business, because you have indicated that you do not encrypt; it is done at either—

Ms Salier—In terms of being an ISP, but now we are moving in terms of being a content hoster. I can take that question on notice and come back to you on the cost of encryption keys. Encryption is not really a complete area of expertise of mine, however I am happy to come back to you on that question. I would need to consult with colleagues.

Senator GEORGE CAMPBELL—Why do you say it would cause a loss of consumer confidence? Is it just a guesstimate? The fact that you can now get listening devices on telephony and telecommunications systems does not stop people using the telephone.

Ms Salier—Yes, but the telephone does not give access to as much information as the Internet does. In a telephone conversation that is intercepted, you intercept one conversation on

one topic. It is just one medium of communication point to point. When you are intercepting communications on the Internet, you are talking about intercepting web sites that are visited by people, you are talking about intercepting chat sessions that are had by people, you are talking about intercepting emails. There are myriad forms of communication that take place over the Internet which make it not analogous to a telephone conversation.

Senator GEORGE CAMPBELL—But I assume that 99 per cent or 95 per cent of the people who use it use it for honest purposes and would not be concerned about any implications of being listened in to. It is the five per cent that are using it for other purposes that you would cause a loss of confidence with. I am just wondering why you make the statement. Have you surveyed customers?

Ms Salier—Yes.

Senator GEORGE CAMPBELL—Have you talked to customers about this?

Ms Salier—I can certainly provide information to the committee on surveys that have been done in Australia and overseas, undertaken by research analysts such as Forresters, which, over the years since the Internet has been a rising medium, consistently show that reticence of embracing the medium by users largely rests on privacy and security concerns.

Customers out there are concerned about their privacy; even the 95 per cent of honest customers are concerned about their privacy. For example, it would certainly be accepted that there are certain pornographic activities which are illegal, but there is a whole range of pornographic activities that are not illegal. There are certain sites which are just R-rated, and you can go through them by age verification procedures and there is nothing wrong with that. But that does not necessarily mean that Mr Honest Citizen, who happens to have an interest in that particular area, wants to be surveyed.

Mr KERR—No, indeed. For example, if they subscribe to *Penthouse*, and presumably *Penthouse* has a list of subscribers and privacy principles govern that you are not supposed to release it, so that the fact that –

Senator GEORGE CAMPBELL—Or if they make those 005 calls.

Mr KERR—There is billing information about that. It is held securely and presumably there are rules about its access and release. People undertake these transactions all the time knowing that if a person of bad faith got access to this information, that could damage them. It is one of the unavoidable consequences of dialling 005 numbers, I suppose, and you hope that it does not happen. What is the difference in your environment? Yes, it is true that some people might prefer that such an opportunity could not possibly arise, but they undertake these kind of risks with all kinds of behaviour all the time.

Ms Salier—I come back to the surveys that show that people do not use the Internet right now because of privacy concerns. As I say, I am happy to provide those details.

CHAIR—Is that privacy or security?

Ms Salier—Privacy and security and the security concerns that they are worried about are not so much, 'Am I going to be attacked by a virus?' They are more along the lines of, 'If I put my credit card on the net is it going to be' –

Senator GEORGE CAMPBELL—We all have that angle.

Ms Salier—That is right, which again emphasises the importance of using encryption.

Mr KERR—Going back to people who subscribe to 005 numbers or buy *Penthouse* or what have you, in the past there always had to be a billing record somewhere. You can now subscribe through an Internet system, presumably where you say the only information that we are going to hold, at most, is the fact that you logged onto OzEmail and you logged out of OzEmail at such and such a time. You were asserting that your system—an ideal system—would have less information than currently exists in relation to human conduct.

I am not trying to suggest that we should move down this track, but I am trying to clarify precisely what it is that we ought to protect because none of us wishes our privacy to be intruded upon; none of us wishes to have our phone calls recorded and none of us wishes to have what we buy known to others. But we accept that, for law enforcement purposes, that opportunity may arise if we become the subject of suspicion. That is just a reality.

Ms Salier—If I can make the point here that the thrust of some of the submissions made to the committee were in relation to retaining certain records, such as the ones that you are describing which are held by ISPs. The point that I made during my opening statement was that we retain certain records right now which is for legitimate billing purposes—you need to know when people log on and log off so that you can add up their hours and charge them their hourly rate, their plan or whatever they are on.

I guess I am moving beyond the realm where there is a call for regulation of what records should be retained by ISPs. I am saying that, as a general rule, there should not be an obligation to retain the sorts of records that we are discussing here, namely, when you log on, where do you go? Just as there is not a general obligation on Telstra to record anything beyond the fact that the person dialled from here to there—unless, and again I come back to the interception warrant, there is a specific requirement placed on a carrier to do so.

CHAIR—Can I clarify, is your objection because you think that that information should never be made available to law enforcement people—given appropriate suspicion and the issue of warrants and all that sort of thing—or are you saying that it is a purely logistical and cost thing?

Ms Salier—No, I am saying that that information should only be available under a strict checks and balances policy where the rights and privacy of the citizen involved are looked at and protected before such –

CHAIR—But, if I am a person engaged in criminal activity—and given that I can use the Internet in a way that I cannot use the telephone, because it is multipoint and all that sort of thing—are you saying that ISPs should not keep track of what I do and that that not should be available under appropriate legal protection when I become a suspect and the warrant is issued?

Ms Salier—It currently does though. There is a general obligation on ISPs to have an interception capability under the Telecommunications Act. So that currently exists without having to lift a legislative finger, so to speak. We currently have this general obligation. Carriers, of course, have a higher level of obligation where they have to put in an interception capability plan and ISPs do not. But, nonetheless, the general obligation to provide an interception capability rests upon carriage service providers, as they are referred to in the act, which includes Internet service providers. So in fact the situation that you are referring to there—where there is an investigation of a person suspected of whatever and then there is a requirement to intercept communications in respect of that individual—is already covered under the act.

Senator GEORGE CAMPBELL—Is your argument really about access, in terms of access to other individuals?

Ms Salier—There are two separate issues here: there is the interception issue and there is the retention of records issue. The interception capability is dealt with under the Telecommunications Act. We have the Telecommunications (Interception) Act, which clearly sets out how, when and why a warrant will be issued for interception of communications. The issue that was of grave concern to the IIA from the submissions really related to the fact that there were several agencies that appeared to be calling for the general retention of records such as would only be ordinarily retained in the event of an interception warrant.

Senator GEORGE CAMPBELL—I am trying to get to what the IIA finds acceptable in the way in which this ought to operate. You have spent a lot of your submission this morning dealing with other submissions that have come before the committee and have pointed out some of the dangers that are inherent in the ASIC submission, et cetera, but you really have not put on the table for our consideration how your ISPs view this issue and what you think would be a reasonable regime in terms of access.

Ms Salier—The IIA believe that the co-regulatory regime can work in Australia and that we should be working with law enforcement agencies to ascertain exactly what records they are asking us to retain and have access to under the more general power of section 282 of the Telecommunications Act. We believe that, once we have the discussion with the law enforcement agencies, we will find that the agencies and the industry are not that far apart in what records can be provided and what records are actually being requested.

Senator GEORGE CAMPBELL—Would the National Office for the Information Economy be an appropriate body to conduct discussions with the interested parties to try to work out a regime that would be acceptable?

Ms Salier—We would prefer it to go through the Internet Industry Law Enforcement Taskforce that has just been set up for the very purpose of having these discussions with law enforcement agencies.

Senator GEORGE CAMPBELL—Who set that task force up?

Ms Salier—The Internet Industry Association has set that up. It is being chaired by one of its directors, Justin Milne, who is the CEO of OzEmail Internet. We have been talking to the law

enforcement agencies throughout the period of the Internet Industry Association coming into being to try to work out what they want, what we can give them and how we can allay the legitimate concerns of law enforcement agencies while fostering the growth of our industry and making sure that people still have confidence in the industry in order to come online, embrace the industry, use it for e-commerce and so forth.

Mr KERR—I am trying to get a fix on where we are at, because in the telephone interception environment at the moment you can get two classes of information. You get real-time information—that is, if you get a warrant you can hook in and intercept anything that is done on that service for the time for which the warrant operates. You can also get billing charge information, which gives you who spoke to whom at what time in the past. Taking Senator Campbell's point, if you pick up the phone now and you use it, you know that if there has been a warrant issued it could apply to that call you are making and, even if it is issued now, it can also mean that it can reach backwards in time to get a list of information of who you were speaking to at what particular time.

The problem with the Internet industry is that you say that you can have real-time contact in the future if you get a warrant, subject to the fact that a lot of this stuff is pretty highly encrypted and very difficult for law enforcement to break into—pretty good privacy is still pretty good privacy as far as criminals are concerned—but there is no equivalent record of who did what and made what contact with whom. In other words, that piece of law enforcement information that is available on phone systems is not available because you say, 'We don't hold those records and we don't want to.'

I am asking you, if you are trying to do the equivalent, and we move past the point where real-time interception really matters in this digital age, why we cannot set a period of time where that kind of equivalent information can be lawfully sought. I am asking that question because it seems to be an obvious one to us.

Senator GEORGE CAMPBELL—I thought Ms Salier said earlier that they do keep billing records.

Ms Salier—There are a number of issues involved in that as well. Our billing records will show, as long as we have the user ID. For a start, often police investigations start with an IP address as opposed to a user ID. Therefore, you have to work backwards to find out who you allocated the IP address to and at what time in relation to user records.

The other issue is that currently we cannot get access to caller line identification – CLI – from Telstra. We record caller number display when it is offered, but we cannot get access to CLI in order to be able to identify the phone number from which every user dials us at this point in time, which can inhibit some investigations as well, if you are looking for a spot that the user is sitting in.

In relation to your question, I have to go back to the issues that I have already raised. There are privacy issues and there are cost issues. Under the Telecommunications Act we have an obligation, like the telecommunications industry in general, to maintain privacy of that information. The information that we are talking about collecting here is of a much greater magnitude than in point-to-point conversations. I would say that the analogy, as I said in my

opening statement, is not the difference between getting access to who went where and did what. That is akin to recording a telephone conversation every time a conversation is made. We can tell you when one of our users has been using our system, just as Telstra or a carrier can tell you when one of their users has made a call, but I believe the next step is actually akin to requiring a carrier to record the conversation.

Mr KERR—Let us see whether there is a middle ground—and I do not know whether there is. Is there a middle ground which would require you to track, not to copy every communication necessarily, but to have the same kind of information as to where users actually go in terms of their contacts within their use of time that is blocked out to them?

Ms Salier—I would say that, in the online world, that is akin to recording a telephone conversation. There is no difference.

Mr KERR—There is a difference. If you are recording—

CHAIR—If I send him a message on the Internet, there is a difference between recording the message I send him and merely recording the fact that I entered the Internet and he was the recipient of my communication. If you know that I sent a message to Mr Kerr, that is the same as knowing that I made a telephone call to him. It is not the same as actually recording the content of the communication.

Ms Salier—I guess we need to come back down to technical capability as well then in terms of that particular thrust of where it could potentially go. At the end of the day, it is not a point-to-point communication, so therefore you could get on the Internet and you could be going to Russia or you could be going to the email next door or whatever. We do not have the technical capability right now in order to track that information and there would be an enormous cost. As you can see with the RIP Act, that is essentially what they are legislating for in the UK. The British Chambers of Commerce report, which I will leave you a copy of today, indicates that the cost to the nation is billions of pounds, and the cost to the industry is millions of pounds. At this point in the economic environment, I think that it could be the end of the industry.

Mr KERR—The cost of fraud to the Australian community now would be probably 15 to 20 times what it would cost Britain in terms of the installation costs. The sort of numbers we are talking about that are avoided in the tax system, that are laundered illegitimately, that are taken out of companies for fraudulent purposes in both the private and the public sector, are just huge.

CHAIR—I think the salient point is that whilst that may be the case globally, she is worried that the actual cost of doing something about it is going to be borne by her industry.

Mr KERR—Absolutely, but this is the same argument that telephone companies put up every time they have to provide encryption to governments so that the AFP and others can access telephone tapping. It is a cost that industry sometimes bears. I am not trying to suggest that we should necessarily do this, I am just trying to get a fix, because I think that there are very serious issues. I think that the privacy issues you raise are significant because if you were storing that much information, the chance of leakage is possibly reasonably high and has to be taken into account. People might be frightened that a whole range of personal communications, private communications to their girlfriends and what have you, might at some stage be released.

I think that is a quite appropriate thing for us to be very rightly concerned about. But on the other hand, I do not want us to get into a situation where we say, 'Hang on. We can't find methods of allowing effective law enforcement into an environment where law enforcement expertise is slight and where crime is likely to burgeon.' It has to be efficient. It has to be something that can be done. You cannot just leave it and say, 'The poor old law enforcement officers already have the tools and capacity to do it with,' because they do not; they are hopeless in this area.

Mr SCHULTZ—Just on that point, this begs the question: could criminals establish an ISP through which they could safely route all their communications? Given the significant major challenge that we are facing in the future with regards to money laundering on the Internet, how do you address these two particular problems?

Ms Salier—I am going to have to take that question on notice. I have to say that in my experience with cybercrime, I have never had anything to do with money laundering. I am happy to go back and consult with my colleagues and come back to you with an answer on that question.

Mr SCHULTZ—But that question directly relates to the concerns being raised here about the privacy issue that you are talking about. That is why I asked the question.

Senator DENMAN—You are talking about black money, are you, from crime? Is that what your question is?

Mr SCHULTZ—Yes.

Senator DENMAN—I was going to ask that.

CHAIR—If there are no further questions, I thank you very much for coming this morning. It has been a very interesting session. You are going to take a couple of questions on notice and you are also going to supply us with some further documentation in the fullness of time. We will send you a copy of the transcript of your evidence to which you can make alterations in respect of specific error. Thank you very much indeed for coming today.

[10.37 a.m.]

BERRIMAN, Detective Inspector Stephen John, Officer in Charge, Technical Support Unit, Victoria Police

LEANE, Inspector Stephen Frederick, Manager, Legislative Review and Proposals Unit, Victoria Police

CHAIR—Welcome. We have received the Vicpol submission—forwarded by Commander Paul Hornbuckle, the Chief of Staff, in August last year—which has been published by the committee. The committee prefers that all evidence be given in public, but you may at any time request that your evidence, part of your evidence or answers to specific questions be given in camera and the committee will consider any such request. Would one of you like to make an opening statement before we go to questions?

Insp. Leane—Yes, I would like to make a brief statement. I am Manager of the Legislative Review and Proposals Unit as stated. Part of my role is to prepare responses to committees such as yours and also to make proposals, as the name says, to the Victorian government in relation to legislative change. The reason Detective Inspector Berriman is here, and he will explain, is that he is an expert in the area of electronic surveillance, for want of a better description, and he has been in his position for somewhat longer than I have been in my position. So perhaps Mr Berriman can introduce himself and then we can answer any questions.

Det. Insp. Berriman—I am responsible for covert technical operations of Victoria Police and the management and coordination of operations under the state Surveillance Devices Act. The state Surveillance Devices Act was enacted in January 2000, as I think you are aware. Prior to that we operated under the Listening Devices Act, which solely dealt with audio surveillance. It came in during 1969 and it was silent on issues such as electronic tracking, data surveillance, tracking the use of optical surveillance devices and certainly the wider use of listening devices.

It took 30 years to gain new legislation in what we would see as an important area of police use of investigative technologies. The challenge for us was to deal with the new and emerging investigative technologies, the developments in surveillance devices, while still falling within the restraints of the Listening Devices Act. The technologies that were outside that act and essentially had no legislative control presented us with a great dilemma. There were great possibilities for us, great opportunities, yet the ability to work with these new tools—they are not only available to us; they are available to the wider community—was denied us. There were some serious risks in exceeding what were the legislative bounds of the Listening Devices Act and certainly the more traditional bounds, such as trespass to premises, unlawfully on premises and the restraints that were imposed there.

The challenges for us in the next decade are to harness the new levels of technology that are coming on board, and they are coming on board at an increasing rate. A further challenge is to gain cooperation and support from industry, commercial vendors and companies that used to be government departments. Essentially these corporations have wider interests than serving the community of Australia and they have responsibilities to their shareholders and their corporate

groups. We have found in recent years there is a serious conflict between those companies discharging their commercial obligations and meeting the community interests, the community expectations, and the public responsibility served by law enforcement.

The Surveillance Devices Act—and we have made comments about that in the submission—legislated in section 22 to provide an assistance order. That assistance order is very much drawn from the Canadian criminal code as it relates to police use of electronic surveillance, and those provisions are virtually identical. This experience we are facing in Victoria is by no means isolated to our state. It is common, and it is common throughout the Western world. I have direct experience from that as I represent Australia and New Zealand in an international cooperative forum amongst law enforcement agencies, which involves technical surveillance specialists.

We have found an increasing reluctance on the part of commercial industries to support law enforcement in their investigations. I can appreciate that often they have a fiscal responsibility to an individual or a company. We will use the example of the previous witness. If I were to sign on with an Internet provider, be it OzEmail or anyone else, by giving them my money I would expect a degree of privacy, as the Chairman pointed out, against my credit card details being passed around, or against some unlawful interception. I pay money for that.

I think the assistance order under section 22 of the Surveillance Devices Act in Victoria will provide corporations with some protection against civil redress by a claimant and that they have an obligation to assist law enforcement in a particular case. I will give you an example of a recent experience we had. Victoria Police had taken a proactive measure to approach commercial companies for assistance and outline the scope of the assistance that we are likely to expect in the event of a surveillance device operation. Given that most of our work involving the police use of surveillance devices is targeted at major crime—and increasingly we are getting more involved in, and reacting to, specific crimes—the majority of our work now is involving offences such as armed robbery, homicides, aggravated burglaries and sexual offences—a lot of offences that actually have been committed. If we were to approach a telecommunications carrier or a company or the local corner milk bar and request assistance, it is to our advantage to have briefed those people and to be able to talk through the issues and the type of assistance we wish to provide, rather than go there in an emergency situation and expect to get a full and adequate response from an individual or a company.

One company in particular, an Australian manufacturer of a high security locking system, responded with a point-blank, ‘No, we don’t wish to assist.’ We outlined that what we really wanted to find out was enough information to enable us to do our task without approaching that company and asking them specific details about specific clients, and placing them in a position where they are giving very pertinent client information. We wanted an overview, if you like, of their systems and their approaches to enable us to do our job. The company came back with a no. When pushed further, they threw a figure of quarter of a million dollars and said, ‘That is the sort of money we would want from you each year to enable us to give you that service.’

We are faced with risks of commercial-in-confidence, which is a serious thing for a company that has put a substantial investment into product development, and we can appreciate that. We frequently use deeds of confidentiality and non-disclosure which are signed by the state minister, and they place the company in a position where, if information they do provide us gets

out of the police circles, there is a remedy for them. This document is frequently used. Are there any other issues you would wish me to explore?

CHAIR—One of the things we find interesting, given that our prime interest is the operations of NCA—although we obviously acknowledge that it has wider implications than that—is what happens with your surveillance devices in terms of cross-border/state activity.

Det. Insp. Berriman—The cross-jurisdictional use is a significant concern. At this stage, legislation restricting the wider use of surveillance devices—that is, the four technologies that I mentioned—is really confined to Victoria, Western Australia and the Northern Territory, the Northern Territory having come on board late last year. The legislation is similar. Our concern is that if we place a tracking device on a vehicle in Melbourne, or we place a listening device on a person, we will not then have control of that device. Often the device can move outside the jurisdiction of Victoria, outside the scope of the legislation, where it is not within our knowledge. I am somewhat reluctant to go into the specific details of how the technologies work, but if that would assist I would be happy to do that.

CHAIR—Would you prefer to do that in camera?

Insp. Leane—We would.

Mr SCHULTZ—Why is there a reluctance by states such as New South Wales to match that sort of technology tracking with Victoria?

Det. Insp. Berriman—The New South Wales police are very well developed in their equipment and resource base for electronic surveillance. Their legislation is virtually what Victoria's was prior to 1 January 2000. They have made some minor amendments, but they have been as a consequence of adverse findings in criminal trials. The legislation in Victoria, let me say, was developed in consultation with all stakeholders in Australia. Through the ACPR electronic surveillance program, we circularised the issues and a series of 17 recommendations were developed. They were supported by each federal and state jurisdiction in Australia, including the National Crime Authority. There are other stakeholder groups such as the integrity units in New South Wales and Queensland. That legislation appears to have had varying degrees of support or acceptance across Australia. I am aware that a number of jurisdictions have put it up only to find difficulty with that. I am not sure of the exact reasons for that. In Victoria, the Attorney-General at the time, Mrs Wade, certainly gave very good support to the legislation, and we got ours up quite as much as we asked.

Mr SCHULTZ—You are saying that in conjunction with other states—I presume through the police services—you compiled legislation which they were agreeable with but which was overridden or made difficult by the powers that be, either of a political nature or whatever?

Det. Insp. Berriman—Mr Schultz, to be specific, I am not sure of the results after they left the police service. I can only say that, amongst the technical surveillance groups, there is a cooperative professional body around Australia, and after consultation with their end-users, that is the criminal investigators and the operational police, the 17 recommendations were found. How it went beyond their police services I am not sure.

CHAIR—We will keep going in open session and then when we finish the open session we will go into camera to deal with specific issues. The Deputy Chair and then Mr Hardgrave.

Senator GEORGE CAMPBELL—You say that there has been collective consideration of the legal and constitutional impediments that exist within Australia to law enforcement, and that you have got 17 recommendations sitting somewhere as to how you address those—

Det. Insp. Berriman—Yes.

Senator GEORGE CAMPBELL—but they have not gone beyond, presumably, recommendations from this task group?

Det. Insp. Berriman—No. In Victoria they formed the basis of the submission to the state Attorney-General for review of the Surveillance Devices Act. The same occurred in Western Australia. I am aware there was close collaboration between the Attorney-Generals' departments in Western Australia and Victoria. The same legislative framework was developed in the Northern Territory as well.

Senator GEORGE CAMPBELL—Do you know if they have been subject to a meeting of the ministerial group that covers the Commonwealth minister and state A-Gs?

Det. Insp. Berriman—The APMC I believe was made aware of the issue and the need to seek a common approach to legislative reform in the area of electronic surveillance.

Senator GEORGE CAMPBELL—And you do not know whether or not they have considered that or if there has been any outcome?

Det. Insp. Berriman—Other than to resolve that there did need to be a common approach. A useful example is the Victorian and Western Australian acts. While they looked at the same principles, the way they were drafted is a little bit different and there are some principles in the Victorian act that were not adopted in the Western Australian act. The Western Australian legislation has some principles that are not in the Victorian.

Senator GEORGE CAMPBELL—Are they different for the sake of being different—or are they issues of substance?

Det. Insp. Berriman—I am probably not qualified to answer that, Senator. There are certainly questions of drafting style. On some issues they are different in terms of substance. The Victorian legislation has, under section 25, provisions for the emergency authorisation of the use of surveillance devices, typically in siege hostage situations where there is a requirement for an immediate response. The Western Australian legislation approached that differently—I think it is under section 16—where there can be, if you like, a retrospective sanction of the use of the surveillance device, where someone has used it in the public interest. That certainly applies more widely than two law enforcement agencies.

Senator GEORGE CAMPBELL—In the Victorian government submission they refer to the police commissioner's electronic crime working party which it says 'constrains some of the

problems surrounding international cooperation in the area of computer crime and criminal law, including mutual assistance applications.' Has this working party concluded its work?

Det. Insp. Berriman—I am not fully aware of that other than to say the Australasian Centre for Policing Research did a paper on electronic crime. It was a scoping paper and it was done under the sanction of the commissioners of Australia and New Zealand. That paper, I understand, has been prepared and has been circularised.

Senator GEORGE CAMPBELL—Can we get copies of that?

Mr HARDGRAVE—You said before that a proposal has been put up. Do you mean: put up to the parliament or to the head of the police forces? Where is this falling down? Is this all jurisdictional jockeying, patch protection, the traditional sort of post-Federation game of New South Wales must be right; Victoria has got to be wrong, Queensland is a different case, whatever? Is that what the problem is?

Det. Insp. Berriman—I am not exactly aware, Mr Hardgrave. The area I have responsibility for is the coordination of a national program under the Australasian Centre for Policing Research. It is a professional body looking at skills enhancement and an approved medium for exchange. We are the service providers, if you like, to law enforcement. We were really harnessing the opinions of our client base and forwarding those to management. In Victoria, that management was receptive to those arguments.

Mr HARDGRAVE—Has it got up in all the other states, and they are not so receptive?

Det. Insp. Berriman—It has gone up to the board of control of the ACPR, which is all the commissioners. It has gone up through minutes of working groups in police technical surveillance, and it has been received well, certainly, in three jurisdictions. How it is achieved in senior police management in those other jurisdictions, I am not aware and I am not aware how it is received at a government level.

Mr HARDGRAVE—We can deliberate on that as a committee, but it just strikes me that this is a borderless area of activity and this process is just making it easy for the bad guys.

Det. Insp. Berriman—It certainly does.

Mr HARDGRAVE—Is it the case, though, that if they skulk across the border, the Feds could get involved? Could you ring up the NCA and say, 'Look, this has been occurring, but now they have moved to South Australia or they have gone to the Gold Coast?'

Det. Insp. Berriman—If the warrant is obtained in Victoria and it is for an offence that falls within the scope of the Victorian jurisdiction, then the most appropriate vehicle is the state's Surveillance Devices Act.

At a federal level, there are limitations on the scope of the Customs Act. If we were investigating an offence of murder we could not use the provisions of 219B—the electronic surveillance provisions of the Customs Act, nor could we use the AFP Act. So we are really in a position where we have to get a cooperative approach. Between the states, in terms of investiga-

tions, certainly from my point of view and with my counterparts in other states, there is no problem at all; there is a high degree of cooperation. But the legislative constraint is, for example, if we are in Wodonga and they cross over to Albury, we are into a different jurisdiction.

Mr HARDGRAVE—So it is as bad as the three or four gauges of rail system a hundred years after Federation?

Det. Insp. Berriman—That is a very good analogy.

Mr HARDGRAVE—Technology is driving this debate fast. It is very difficult, as legislators, to keep up with where technology is taking us. I was reading the latest Australian issue of *Practical Computing* magazine yesterday. The article was all about I Spy which tells you how to protect your computer systems from all of the technology that is available to invade your computer systems. It strikes me that rank amateurs and bad guys have got more tools of the trade than the police.

Det. Insp. Berriman—That is exactly right. I am familiar with that issue. Law enforcement has a great degree of difficulty in dealing with the types of equipment that are described in that issue. In respect of the borders, it is not technology that is causing us the problem. We have a great armoury of resources at our disposal in terms of electronic surveillance. While we certainly have the legislation, we accept that the legislation will not keep pace with the developments in technology because there have to be safeguards of privacy and intrusion considered.

Mr HARDGRAVE—Only for the people who do the right thing, though.

Det. Insp. Berriman—Yes.

Senator GEORGE CAMPBELL—I understand that argument. It will never keep pace with technology; it will always be trailing behind. Why can we not overcome this border issue?

Senator DENMAN—Because we have got states.

Senator GEORGE CAMPBELL—That seems to be an issue that ought to be overcome.

Det. Insp. Berriman—The border issue could be resolved. For Victoria it is not crucial at the moment because South Australia and New South Wales do not have legislation that prohibits the wider use of electronic surveillance; as soon as they do there will be significant problems for all jurisdictions.

Mr HARDGRAVE—Do they understand that? Do you explain that to your New South Wales counterparts? Surely the police services are there to enforce the law—we understand that—but also senior members must be giving advice back through to ministers and so forth.

CHAIR—As I understand it, Detective Berriman is telling us that he does not have a problem with his police counterparts.

Mr HARDGRAVE—But are they explaining that up the line? That is all I am wondering. Are we aware of that?

CHAIR—How his colleagues are explaining it up the line in their jurisdiction is probably not something he is able to comment on.

Senator GEORGE CAMPBELL—We as a committee ought to take steps to contact the APMC.

CHAIR—Abolish all state governments and have one national government—I agree!

Senator GEORGE CAMPBELL—We have been on that track for 100 years. What I am suggesting is that we ought to contact the APMC and ask why that issue cannot be addressed.

Mr HARDGRAVE—There is one point of comparison that might be worth trying to work out. What about cooperation with overseas? Are you finding that jurisdictional differences are not as big an issue outside the country as they are within the country?

Det. Insp. Berriman—The level of overseas cooperation at a technical operations level is very good. There are international bodies similar to the program I described under the Australasian Centre for Policing Research. It is made easier because there are not the same legislative constraints. But certainly, as we move into the wider use of the Internet and the next generation of the Internet, and as we move into the wider use of satellite communications, interceptibility will occur. You may be familiar with the Iridium system that is still up there—the ground station for Australia was not located in Australia.

CHAIR—I thought Iridium had gone bankrupt.

Det. Insp. Berriman—Iridium is still up there, but it is not being used commercially, I understand, at this point in time, until an assessment is made of its viability.

Mr HARDGRAVE—There is a comment in the Victorian Police submission—that is Inspector Leane's area, I suppose—about future trends, electronic cash and banking, money laundering, and online financial services. You observe that there is a lack of banking regulation—I hate to be pedantic—and then two sentences later you say that the banking sector is becoming more heavily regulated, which I do not think anybody believes is the case. Are you actually advocating the need to look at the use of the online economy in a far more determined way to follow the transactions far more closely than is the case?

Insp. Leane—You were probably not present for the previous submission by a lady who was on the adverse side, and it is difficult for Mr Berriman, who obviously has a vast knowledge of a lot of things in electronic surveillance but not computers. We have a problem, as is displayed within the submission, with staffing of our computer section and we effectively make the submission that we cannot keep up from a state organisation perspective. We have a lot of trouble not in training our people, but in keeping them.

Senator GEORGE CAMPBELL—Commercial work pays too much.

Insp. Leane—E-commerce and the corruption of e-commerce are not just a problem for law enforcement. The last three managers of our computer crime section have all gone on within very short time periods. Sworn members of the Victoria Police have gone on to private enterprise. That is the difficulty we face, so we are some way behind, which is the thrust of our submission.

Mr SCHULTZ—Correct me if I am wrong, but we have just established that the biggest single frustration from the Victorian point of view are the legislative impediments on a state-by-state basis that have created that stopper which concerns all of us. Is that similarly the case with the Australian Federal Police? Is the Commonwealth legislation also creating that sort of an obstacle in your cooperation with police at the federal level on those particular issues?

Det. Insp. Berriman—No. The AFP act of 1979 has specific electronic surveillance provisions, but at this stage they are restricted to the use of listening devices. It is silent on the use of other technologies. Where they are investigating Commonwealth law, they do not fall within the provisions of the state legislation; that is, they do not contravene the state legislation, certainly in Victoria, and the case is the same in Western Australia.

The impediment for installing tracking devices at a federal level is the issue of trespass re-entry. There are some very sophisticated technologies available which are dealing quite adequately with the present problems and there are good future projections for technology development to assist us in that area. There is legislative support to actually place a device on a vehicle or an object, and for the entry to the vehicle or entry to premises to install the device , but there is no legislative support for entry to premises to retrieve it—and it may not be the same premises. Once you placed these devices, particularly in a mobile environment, you have to have contingency plans to retrieve it. You have to have contingency plans to do that safely. That is not possible without legislative support.

Mr SCHULTZ—How do you overcome the situation where, as an example, you get a courier taking cocaine from Melbourne to Sydney and you have a courier taking heroin from Cabramatta in New South Wales down to Melbourne? How do you overcome those problems?

Det. Insp. Berriman—I am trying to alert the committee to the issue as legislative support develops in all jurisdictions. At this stage, we would take out a warrant in Victoria under the Surveillance Devices Act for a tracking device. We would move that. Once it hits the border, it goes into New South Wales. The New South Wales legislation is silent on the use of tracking devices at this time, so there is no prohibition. We have entered the vehicle in Victoria lawfully. It goes to Sydney and, as is frequently the case, the drugs come up or the money goes up and the drugs come back. It is a case of the legislation in New South Wales being silent.

Mr SCHULTZ—So the vehicle could be lost for the distance between Albury and Sydney because they cannot track it?

Det. Insp. Berriman—No. We can still track it. The legislation is silent in New South Wales as to whether you can track it or not.

CHAIR—The point he is trying to alert us to is if New South Wales were to introduce legislation to prohibit the use of these particular devices, then you would have a real problem when you crossed the border.

Det. Insp. Berriman—Then we would commit a criminal offence without a similar warrant in New South Wales. To dovetail that, we may get information that he is going to Wangaratta—and these are actual circumstances—but he does not go to Wangaratta, he goes to Wagga. Under the next generation of legislation, when New South Wales has it in place, we would commit a criminal offence when it hits the border and moves into Albury.

There is that issue, but there is also the risk of loss of evidence when a court has to adjudicate on the prohibitive and prejudicial value of evidence and the compliance with legislation. They are increasingly less likely to take the police view that, in essence, we were doing the right thing. There is a more strict interpretation on the admissibility of evidence than probably there was in times gone by. It is not a satisfactory position, we would suggest, to place criminal investigators in, because there is then an individual liability on the member for doing that.

In our submission, the issue could be satisfactorily dealt with by creating extraterritorial provisions under the respective surveillance devices legislation. The provisions would recognise a warrant allowing the installation and use of such a device in Victoria—if it is created in Victoria—and, by virtue of the extraterritorial provisions in New South Wales and in other jurisdictions, the provisions would recognise the installation, use or retrieval of the device in that jurisdiction.

CHAIR—On the evidentiary front, perhaps you could comment on some of the new evidentiary problems that technology provides. I am thinking in particular of digital cameras where, obviously, it is much easier to manipulate the photograph than in some of the more traditional photographic techniques.

Det. Insp. Berriman—It most certainly is. This is an issue with optical surveillance devices. It is also an issue with audio surveillance. We are in a digital era, but from a law enforcement perspective, there are certainly some significant traps in respect of providing an audit trail.

The House of Lords in the UK did a review of digital evidence, and they basically said—and this is my summary; it is probably not a legal summary—that issues such as continuity and the traditional evidence of continuity should be observed. Electronically, I think we can do a little bit better than that. Some of the systems we have sought to develop have an audit trail in them—there is a verifiable account of what has actually been done to the recording. It is taking it from a recorder and burning a CD with it, and that being able to be traced on a track on the recording, and, if any subsequent copies are made, that audit trail being transposed. That is a lot easier to do with audio than it is with video. It is all data and it should all be able to be managed the same way, but there are some other problems with that.

Mr HARDGRAVE—Does digital technology not mean that in fact the data is accounted for; that is, 24 frames per second, it has a certain data identity as it goes through, and each frame—each second—actually is encoded into the tape? Digital technology, I would have thought, actually enhances whether anything has been tampered with or otherwise, but maybe I am wrong.

Det. Insp. Berriman—That is certainly the theory, but there have certainly been some counterarguments placed in criminal trials. We are looking at possible arguments that may come up. It is a diversion—it can be an obstruction—but there is a possibility with digital recordings, particularly audio recordings, to alter and for that to be quite difficult to detect.

Mr SCHULTZ—Would you like to make some comments about the operations of the Surveillance Devices Act 1999? In practice, would it make a suitable national model? Could you outline the privacy safeguards built into the legislation? In other words, have there been any privacy difficulties for Victoria Police to date?

Det. Insp. Berriman—Section 36 of the act relates to the destruction of records and the control of records. We have not had any privacy issues or intrusion issues with this legislation, nor, might I say, did we have it with the previous provisions of the state Listening Devices Act. The legislation requires that the material be kept secure, and it places that obligation on the chief law enforcement officer. In the case of Victoria, that is the Chief Commissioner of Police; in the case of the National Crime Authority, who have operations under this act, their chairman has that responsibility, so it is then a delegated responsibility.

In Victoria, we require that a particular case officer is appointed. We have a policy and standards manual on electronic surveillance services. That document requires that the case officer keep secure all the transcripts, all the tapes and all the recordings, and they can be released only in the course of the investigation, for transcription, et cetera, or for delivery to the defence or counsel in the case of a criminal trial. Destruction requirements are stipulated in the act. In Victoria Police, that must be done in the presence of a commissioned officer, and it is done as part of a monthly inspection process. The material in Victoria can be kept only for the prosecution or the decision to prosecute an offence, and there are a number of other actions under the confiscations act. The exception is when it is admitted into court. Once it is admitted into evidence, like any other evidentiary document, the document can be moved from there. The combination of the legislation and the internal policies of Victoria Police, which were explained to the working party during the development of the legislation, appears to work quite well.

Mr SCHULTZ—It would make a good national model.

Det. Insp. Berriman—In that aspect, it would make a good national model. The second part of your question, Mr Schultz, related to the particular aspects of the legislation. There are a number of provisions that we have put forward for amendment. They relate to issues, most of which were agreed to during the working party and were agreed to by the minister. In the way the legislation was led, it was the eighth draft. We did not see the eighth draft until it had come out of parliament, having been passed. There are a couple of ways that it was drafted that made it difficult. We probably could take it to a case of testing it at court. But our reluctance in doing that is that we may well lose the evidence. And as Murphy's law would have it, it would be the evidence you really want to keep that you would lose.

CHAIR—If you ever leave the police force, you would do well in the diplomatic corps.

Senator DENMAN—In your submission, you address child sexual abuse, 'Child sexual exploitation is a burgeoning national and international problem.' Is it increasing or it is perceived to be that way because there is more publicity?

Det. Insp. Berriman—The vehicle of the Internet and the anonymity it creates has increased the problem significantly. There is no face-to-face contact. You can represent yourself as anyone. It is a written document essentially that you are typing. Although there is the ability to have that face-to-face video and face-to-face audio, the more practised offenders in this are really looking at the exchange of material and personal information. This is an excellent vehicle for them to achieve their ends. The international boundaries are just not there. There are no boundaries to that system.

The issue of encryption is a very difficult problem for law enforcement to deal with—not the actual breaking of the encryption or the decryption—but the fact that law enforcement investigations frequently rely on dynamic access to information. In the survey that the Victoria Police have done, that is exactly what our investigators want. With something like child pornography, if he has got it in his computer system and it is sent there, you really need the nexus between an individual and that access to the Internet. The way to do that is when he is there. To do that, you need dynamic access to what he is actually looking at or sending.

Senator DENMAN—How involved is the criminal element in this? What you are describing is a crime, of course. But is there a criminal element behind it?

Det. Insp. Berriman—I have some experience in the child exploitation unit in Victoria Police. The subject of international transfer of child pornography and paedophilia related material is the subject of discussion at the international forum at which I represent Australia and New Zealand. The degree is certainly increasing. The protection that the Internet has given these people is increasing as encryption develops. PGP is a commonly found piece of encryption technology that is freely available. It almost has shareware status. It is off the Internet and that key is extremely difficult to develop. I take it, the committee would have heard of that.

It is also difficult for investigators to get to an individual on the Internet. I know you had some discussion on this with the previous witness. The barrier is the ISP. The closer you move to people, the more risk you take during an investigation that they will become aware. To give you an example of this, in America, the telecommunications industry is unregulated—I do not know if it was ever regulated—but there are literally hundreds and hundreds of telecommunications service providers. In one case on the Mexican border, a group—not a legitimate group—got hold of a local cellular system. If police go to that telecommunications provider and ask for information—it could really just be background information on who is the holder of this cell phone number—your investigation is compromised. It is very difficult dealing with these people where there is no real responsibility for them to comply. I take the committee back to my discussions on commercial interests, commercial vendors, et cetera.

CHAIR—Thank you. If there are no other general questions, we will go in camera for a short while.

Evidence was then taken in camera, but later resumed in public—

[11.30 a.m.]

GAUDIN, Dr John Howard, Legal and Policy Officer, Privacy New South Wales

CHAIR—I welcome Dr John Gaudin. We have received the submission forwarded by our former colleague, Chris Puplick, who is now the New South Wales Privacy Commissioner, which has been published by the committee. Dr Gaudin, the committee prefers all evidence to be given in public, but you may at any time request that your evidence, part of your evidence or answers to specific questions be given in camera and the committee will consider any such request. As a public servant you will not be asked questions which seek your opinion on the merits of government policy. Do you wish to make an opening statement?

Dr Gaudin—Thank you. Privacy New South Wales was established in February 1999 by the Privacy and Personal Information Protection Act 1998. It replaced the Privacy Committee which had existed since 1975. The Privacy Committee had a broad mandate to investigate and research any matter involving privacy which went beyond a narrow focus on the application of information principles to the public sector. We have had an active complaint service, which allows us to monitor privacy concerns in the community, including those dealing with the impact of intrusive technology.

I have been a research officer with the Privacy Committee since 1992, and a legal and policy officer with Privacy New South Wales since December 2000. As a privacy officer, I have participated in research and advice on the New South Wales police records system, the law enforcement access network, DNA forensic legislation, and child protection policies for the New South Wales government. I should say that, as an officer within the Attorney-General's Department, often we are in a position of giving advice and sitting on working parties, dealing with these things including issues such as the working party on search warrants.

Since the commencement of the new act, our efforts have been largely focused on assisting in the implementation of a privacy regime for the New South Wales public sector. We still have the broad general inquiry role, where time and resources allow, but on the whole it has not been a major priority, hence the submission we wrote was possibly a fairly superficial and quick one, trying to address broad general issue rather than getting involved in the details of the kind of technological proposals which we expected to be brought before the committee.

We made some general observations about how privacy should relate to law enforcement. The broad thrust of the submission was a challenge to some recent trends in regulation simply to state that there was a privacy issue, but to broadly exclude it where law enforcement activities took place. We argued in our submission for an overall privacy framework in which law enforcement agencies should be seen as accountable for their actions when they infringed on privacy. This should include the application of a risk assessment approach to assess the privacy impact of various forms of surveillance technology, both from the general and in individual instances.

There is an established tradition of the use of judicial warrants to approve intrusive searches—the use of listening devices and telephone intercepts. In our view, this should be

broadened in a way that establishes more effective safeguards as new forms of surveillance come on line. We would probably say, for example, that the use of traffic data under the Telecommunications Act should be subject to some sort of warrant provision.

Accountability for the use of intrusive powers requires a greater openness than has often been the case. Law enforcement agencies often argue that people should be prepared to trust their high security and confidentiality standards rather than expect specific measures to deliver accountability. My response is that we cannot assume that powers will not be misused. This is not necessarily restricted to conscious corruption, although in New South Wales we have had some instances of this. It can also include overzealousness and impatience with playing by overly formal rules, or the effect of a cultural attitude in law enforcement based on the sense of knowing so much more about the people you are dealing with that you have had the sense of superiority to them.

Another argument put forward by law enforcement agencies is that if the methods of information gathering are too widely known, it will be too easy for wrongdoers to know how to sidestep them. In my view, this argument invites abuse of intrusive surveillance powers. Serious organised crime targets are well aware of what surveillance exists and they are capable of protecting themselves. Covert surveillance then gets used against easy targets—basically, people who are naive enough not to be aware of it. This contributes to the kind of function-creep which seeks to justify the original investment against increasingly petty targets. An example of this in our experience has been the street video surveillance in Cabramatta, which started up being aimed at drug dealing and which ended up being used against minor public order and parking infringements.

A few other issues, I think, are worth putting on the table. One of these is that over the past 20 years since I have been looking at this there has been a general tendency for intelligence based policing. Computerisation makes routine the kind of data processing which was previously used only by specialist intelligence agencies and it has become a normal part of law enforcement. I do not suggest that it is realistic to resist the trend towards this kind of proactive policing when you are targeting people but not necessarily reacting to particular offences, but it does suggest more proactive forms of accountability rather than simply relying on the discretion of judicial officers issuing warrants or the powers of courts to exclude improperly obtained evidence.

Another aspect of openness is the issue of notifying targets once a surveillance exercise is over and using this as a check on misuse. The 1994 Barrett report on the long-term cost-effectiveness of telephone interception gave qualified support to a requirement to notify parties who had been subject to interception warrants once the investigation was concluded. This is standard practice in a number of overseas jurisdictions. The suggestion was strongly opposed by law enforcement agencies and never adopted. We are now witnessing proposals to extend to law enforcement agents generally the powers which ASIO has to hack into people's computers, and still there is no suggestion that there be a regime of disclosure. Currently, all we get for things like telephone interception and listening devices are very sketchy statistics on the extent of their use.

Breaches of the existing privacy safeguards should be treated seriously and not simply as technical infractions. An example of this would be the 1999 case of Takiac v. Australian Federal Police where the Australian Federal Police tried to use intercepts for a disciplinary matter. The

Australian Federal Police lost the case in the Federal Court, but as far as I am aware there was no suggestion that that was treated as an improper use invoking the penalties under the legislation.

One consequence of this is that people who feel they have been subjected to private surveillance get very little support from law enforcement officers. There seems to be a culture, judging from some of the complaints, in the law enforcement community that surveillance is basically a good thing and when somebody other than a law enforcement officer takes undertakes surveillance they find it fairly difficult to actually provide a remedy for the people concerned.

We are concerned about escalating surveillance—the possibility of new forms of technology creating a spiralling of surveillance and counter-surveillance leading to security countermeasures. Again, I think this is a situation where the able criminals are well aware of what is happening and can actually keep ahead of the game if the legal regulation tends to pick up small fry and become a justification for using surveillance for our ever increasing targets.

The existence of intrusive powers with no real accountability fosters a climate in which individuals feel constrained about exercising their normal democratic powers of free expression and association. When I came here, I found myself wondering how many people with real concerns in this area would feel entirely comfortable giving evidence before a committee like this today. I am not saying that the law enforcement agencies go around and monitor people who would stand up against surveillance, but it certainly creates that impression, and from the calls we get from people there is a feeling that surveillance might or can get out of control. So there is another reason that there is a need for a clear privacy framework.

CHAIR—I doubt that you would be under surveillance as a result of today. Anything you have said today you have probably said elsewhere and you would already be under surveillance, if that was the case.

Dr Gaudin—I do not want to get paranoid about it. Certainly a lot of people who ring us up have fallen prey to paranoia about this. You have to sift out those from those who are not.

CHAIR—I take your point.

Dr Gaudin—We owe a duty to the people who are inclined to paranoia to be able to say, 'Well, there are clear legislative safeguards.' I guess that is basically one of the points I thought I would bring up.

Mr SCHULTZ—You gave an example of the misuse of video surveillance in Cabramatta. I was in Cabramatta some time ago and saw the video cameras. I am aware that Fairfield City Council has a significant number of video cameras in their CBD and there are restrictions on the way in which the information on those videos can be used. Can you advise me as to what the restrictions are in terms of a privacy point of view? What are your comments about how that would assist the people distributing drugs in Cabramatta to continue to distribute drugs?

Dr Gaudin—I would not say that the video surveillance system does not assist the police. I have certainly visited the Cabramatta centre and I have audited the use of tapes there. I have observed an intelligence exercise trying to identify dealers there and how that was done by video.

Privacy New South Wales and the previous privacy committee both had a role in auditing the use of equipment. We did find there and in the theatre district, under the surveillance system in the Haymarket, that there was a tendency for the statistics on positive hits or positive identification and wrongdoing there to gravitate towards things like parking infringements.

Mr SCHULTZ—The reason why I asked the question was that I was with another committee and had a meeting with Fairfield City Council. We had to remind Fairfield City Council that as a committee we had certain powers under federal law to obtain copies of the tapes. They were saying that the tapes were not available to be viewed because of the privacy situation. I found that absolutely astounding as a federal member of parliament concerned about the drug distribution in our country.

Dr Gaudin—That system was set up within the privacy policy framework and Fairfield City Council now is an organisation under the New South Wales state privacy legislation. I see that they would have problems or they would see themselves as having problems handing over tapes without knowing that they had a proper authorisation to do so. There was an incident where surveillance tapes from Cabramatta were shown at a conference more or less as a running background to a presentation by a New South Wales police officer which the Privacy Commissioner did object strongly to. I think possibly as a result of that incident which happened about two years ago, the Fairfield City Council may be feeling certainly cautious about disclosing tapes without knowing that it has proper authority.

Mr SCHULTZ—I suppose what I am saying is that if the police had access, and I understand they do in terms of looking at those, can that evidence on those videotapes be used by police to charge and convict a person observed on those tapes as dealing in illicit drugs?

Dr Gaudin—It is my understanding that they could.

Mr HARDGRAVE—I have a couple of quick questions on the matter that Mr Schultz has just raised. In Brisbane in the major mall in Queen Street and also Chinatown in Fortitude Valley—I do not expect you to know either of those areas well—the concept of video surveillance has been in place for a decade or more, certainly in Queen Street Mall. The police run it from a kiosk, and the police use it as a means of keeping an eye on activities, particularly at night, of people congregating and doing mischievous things.

On New Year's day a young chap was brutally murdered and police have been able to get hold of, through those tapes, some people who are helping them with inquiries. I do not know of anyone in Brisbane who complains about this oversight; rather there is a sense of security out of it. I am just a bit amazed to think that police would be concentrating on parking infringements instead of drug deals in Fairfield. Surely, that is spare time activity, if there is such a thing as far as drug deals are concerned in Fairfield or Cabramatta, or wherever it is.

Dr Gaudin—I was using that as an example of the situation. If the law enforcement body invests in an expensive form of surveillance, we justify it usually in terms of some sorts of major crimes. At the moment, a lot of the things that the committee seems to be considering are things like drug dealing, child pornography, tax evasion and money laundering. There is something we see a lot of which the Privacy Commission tends to describe as 'function creep'. Once you have made the investment in an expensive system, then there is a strong tendency to

not only use it for the particular serious offences which justified you buying it, but also to use it to pick up much more minor infractions.

Mr HARDGRAVE—The little old lady getting her bag grabbed in the middle of Queen Street Mall in Brisbane is going to be delighted that the police have got those cameras, because then they can find the perpetrator.

CHAIR—This committee is primarily concerned with the NCA, which covers major organised crime.

Mr HARDGRAVE—I accept that, Chair, but I just think it then goes down the path of what the committee is on about. You mentioned accountability in your opening comments and it seems to me to be obviously the key to this whole matter. Does that then allow you some trade-offs—in other words, accountability of your conduct of the activities you have undertaken with this equipment versus what you have actually been able to achieve versus what else you would like to achieve. Surely openness and accountability may be opening up your files or something for the odd bit of scrutiny every so often. It might in fact be the answer to a lot of these problems.

Dr Gaudin—I would not say opening it up every so often. I think you need a kind of a framework within which your surveillance activities take place. It seems to me that the Victorian police basically described something like that. You have legislation which has a framework which applies to all forms of surveillance and applies fairly similar standards.

Mr HARDGRAVE—So the Victorian model is all right?

Dr Gaudin—I think it is useful to bring this up. We were invited to make a comment on the Victorian surveillance bill when it came in. I do not think we did so. I do not think we had the time to sit down and do that, but certainly they did consult. We would see it as one of our roles to give advice to organisations like that. I think it is probably going in the right direction.

You may be aware that the New South Wales Law Reform Commission has a brief on surveillance and has prepared a report, which is currently before the New South Wales Attorney-General, and which may well cover some similar issues of bringing together the regulation of surveillance. I cannot say much more than that about it at this stage because it has not been published.

Mr HARDGRAVE—At the end of the day, the rules that are in place are only going to be obeyed by law abiding citizens and organisations, aren't they? The bad guys are not going to follow any rules that are in place. They are running around surveilling others, keeping tabs on transactions and knowing what is going on.

Dr Gaudin—What I am saying is that I do not think you can draw a very clear dividing line between the bad five per cent and the good 95 per cent. If your surveillance powers involve, as was suggested by the Internet Association witness, requiring Internet service providers to collect information about transactions on their hard disks for law enforcement purposes, a person who comes under suspicion later on but is purely innocent can also have their transactions looked at and may be shown up in a bad light as a result. Once you actually target a

person, the person can do things innocently but then that information forms part of an overall dossier about them and they can be concerned.

Mr HARDGRAVE—The question of a dossier would not exist if there was openness and disclosure of those sorts of activities after the fact, as you suggested in your opening comments.

Dr Gaudin—I think that is the essence of what privacy is about; people do not like to have all their activities stored up somewhere and accessible for examination. Or if it is going to happen, they want to be sure that there are fairly good safeguards on it—things like warrants, and a requirement to report once the investigation has taken place, so that a person who is innocent and who has actually had their Internet transactions put under the microscope has some knowledge of what has happened.

Mr HARDGRAVE—A devil's advocate, which I am trying to play here, would suggest that 95 per cent want the police to have every possible power to get that bad five per cent, to use your scenario. This bad five per cent is preying on young people with the importation of drugs and is handling transactions of money out the door of this country day in and day out. It would suggest that organisations like yours are aiding and abetting these activities on a daily basis by throwing up all these trips, criticisms and tie-my-hand-behind-the-back approaches to law enforcement.

CHAIR—I think that is rather a long bow to draw.

Mr HARDGRAVE—No, it is not. I am saying that a devil's advocate would suggest that, while no-one disputes the right to privacy, those who perpetrate illegal activities in this country are not entitled to that privacy but are getting it inadvertently by the fact that they want to hide behind one set of rules that guarantee privacy while at the same time breaking every other rule in the book. So where is the trade-off? Where does Privacy New South Wales stand on trying to beat these criminals and stop them destroying so many other people's lives and, in fact, invading the privacy of the 95 per cent as a result?

Dr Gaudin—It is a long question and I will try to answer it. Firstly, the five per cent was a figure used earlier today. I am not sure whether it would be as much as five per cent. Secondly, you made the statement that 95 per cent of the people want this resolved. I would refer to different surveys which have taken place here, in the UK and in the United States which suggest fairly consistently that people's concerns about privacy are fairly high. Something like 20 per cent of the population is very concerned about privacy. Something like 60 per cent of the population has a pragmatic concern about privacy which they will be prepared to waive in certain situations, leaving about 20 per cent of people who are enthusiastic about any justified incursion necessary, whether it protects privacy or not.

We have had protections which have traditionally protected people's privacy. Part of the essence of a democratic society is that you do strike a balance between administration and law enforcement, and getting things done that way, and the state as a protector of individual rights. This is to some extent reflected in the divided ministry position under the federal government and, to some extent, in New South Wales by the division between the Attorney-General's Department and the police ministry.

Mr SCHULTZ—I know that if I did a straw poll in my electorate, 99 per cent of the people that I represent would forgo their privacy, to take the point that my parliamentary colleague made, to address the issue of criminal activity. The Commonwealth Ombudsman has no difficulty with extending electronic surveillance powers to law enforcement as long as they are accompanied by appropriate accountability provisions. Have you got any comment on that?

Dr Gaudin—The third point I was going to make was that in the past we have had search warrants, listening device warrants and telephone interception warrants and we have tended to trust that kind of process. I think if you are going to have a more comprehensive surveillance legislation, say on the Victorian model or on the UK model, you would probably want to look at the capacity of those judicial warrants which are signed on pretty much an automatic transmission belt and maybe have some overall surveillance for those. I guess in the past we have relied on the courts and on the courts ruling evidence inadmissible. I think we are dealing with so much greater an ability to gather data nowadays that we need to have forms of protection actually built into whatever legislation we have, especially if we are looking at expanding to other law enforcement bodies, say, ASIO's power to hack into computers which seems to be on the wish list of most law enforcement bodies that I am aware of. The activity should be restricted to particular serious offences and not necessarily flow on to minor offences and there should be proper reporting, including reporting back to the targets in appropriate situations.

Mr HARDGRAVE—Are we talking perhaps about random computer checking like random breath testing? Random breath testing gets drunk drivers off the roads as statistics show but at the same time it picks up minor offences such as broken tail lights and seat belts not being worn. Are we talking about the same sort of thing as far as technology is concerned? Is that a reasonable step to take?

Dr Gaudin—I would think that the right to privacy is a bit more important than that. Major surveillance powers which involve trawling and picking up any kind of infractions are not appropriate ones to arm law enforcement bodies with. You should have surveillance powers which are targeted to serious offences and, if the people that acquire that information use it for other kinds of offences or other purposes—a classic one is disciplinary matters—the law should somehow record its displeasure.

Mr HARDGRAVE—You are talking about the criminal element hiding their activities within this great range of transactions or this great range of activity on the Internet. That is why I went down this path. Somewhere along the line, law enforcement officers have to have sufficient powers to try and stay at least only one step behind the criminal element, who are always one step ahead of the law.

Dr Gaudin—I do not think I would oppose that. I think the only way in which people will trust that those powers will be properly used will be if they are pulled together in a fairly clearly structured protective framework.

CHAIR—On the one hand, before they are used and, on the other, by reporting after they have been used.

Dr Gaudin—And accountability is a key part to it.

Senator DENMAN—I am not sure whether you have looked at this but I thought of it while these guys were questioning. What about concerns about DNA privacy? Have you looked at that?

Dr Gaudin—Certainly. We made a submission to the New South Wales Attorney-General on the New South Wales legislation. We made a prior submission on the uniform criminal code discussion paper proposing the original Commonwealth bill. I do not think we actually made a submission on the final Commonwealth bill.

CHAIR—We are about to lose one of our number which will make us illegal so I have a motion from Senator Denman, seconded by Mr Schultz, that we form a subcommittee of Mr Nugent, Senator Denman and Mr Schultz. We will have a subcommittee of three but that will enable us to continue with a quorum of two. All in favour? Thank you very much. You now may leave.

Senator DENMAN—Thank you for telling me. Can you just elaborate a bit?

Dr Gaudin—The Privacy Commissioner's major concerns about the creation of a national DNA database were that it would create, unless there were very good safeguards, a tool where it would be fairly easy to put a person in the hot seat and to manufacture evidence linking them to a crime scene, which few defence counsel would have the ability to resist. His solution to that has been the need for an independent body which actually samples and analyses the material before it gets put on a DNA database. I think our other major concern is about creating a database which has differential rules of access for different states and territories.

Senator DENMAN—That is what I was going to ask.

Dr Gaudin—The way the legislation works now, there seems to be an invitation for the lowest common denominator of protections to apply to it. If a state or territory wants to create a situation where DNA evidence can be used basically as a form of identification—a substitute for fingerprints or something—it can be collected in an uncontrolled way and used in ways which are not limited by who is it collected from, but there is a danger there.

Senator DENMAN—This too has a spill-over into gene technology. My concern is that if they start gathering and keeping databases on a person's genetic make-up, insurance companies or prospective employers—those sorts of people—can access all that information. Have you looked at that?

Dr Gaudin—I am not sure whether there is any legal protection against their accessing it. There was the case in Western Australia with the postnatal collection of data, where they eventually had to close down the database after the police imposed search requirements to get that. We have actually been talking to the New South Wales postnatal service on this issue to try and understand exactly in what situations they would actually disclose information or the samples to police.

Senator DENMAN—It is a whole new field at this stage.

Dr Gaudin—I am cautious about aligning the idea of DNA identification, which is about supposedly identifying and linking an individual to a crime scene with a 99 per cent probability, as against analysing blood samples for specific conditions. I do not dismiss the possibility that the two technologies may converge at some time in the future.

Senator DENMAN—That is my concern.

CHAIR—What about other new technologies that are becoming available? As I understand it, if you X-ray somebody's wrist you can determine their age, which was a piece of new information to me. Clearly, it could be quite useful to investigate that at certain times. Would you have a view on those sorts of technologies?

Dr Gaudin—I think it comes back to the normal privacy principles which are enshrined in the federal Privacy Act or in our legislation; that is, if you collect information, you collect it for a legal purpose and you use it for the purpose for which you collected it. I do not see that technology like that, if you have strong reasons for establishing the age of a person, either in a criminal law position or possibly in a migration position, really raises a privacy issue. All you are doing is verifying, presumably, an age which somebody has given or refused to give you. I might be sticking my neck out among privacy colleagues by taking this position. They will probably see the technology as intrusive, but I try to say, 'Set aside the actual usefulness or the ingenuity of technology from the uses to which it is put.'

CHAIR—On that basis would you agree that people should be required to take lie detector tests?

Dr Gaudin—Probably not, to the extent that the privacy committee in New South Wales came out strongly against the use of lie detector tests and actually was instrumental in the New South Wales legislation against it. As the Privacy Commissioner has not made any new policy on that, I would probably have to say, in my official position—

CHAIR—Is it not at variance with your suggestion that you would accept a wrist X-ray that could demonstrate somebody's age?

Dr Gaudin—Yes.

CHAIR—I am not really trying to catch you out; it is a complex area. Similarly, you can get into the infra-red surveillance of dwellings, for example. I suppose one would tend to take the view that if it is properly authorised by the police and whatever, it might be a legitimate tool, but if you or I did it for voyeuristic purposes it clearly would not be acceptable.

Dr Gaudin—And yet it happens—maybe not infra-red surveillance, but there is a constant stream of complaints to us about neighbours using video equipment and people's concerns that they are being filmed inside their houses.

CHAIR—The NCA is exempt from the application of the Commonwealth Privacy Act. Do you have any comment on whether that is a good thing or a bad thing?

Dr Gaudin—I would see it as a bad thing. There is a similar provision in the New South Wales Privacy and Personal Information Protection Act as far as the operational functions of the New South Wales police and other law enforcement bodies go, and in trying to implement the act, I think that that been something of a problem. It is a problem in defining what their operational activities are and how these differ from the educative and administrative activities which are covered by the act. It is a problem for other agencies in working out whether, when they disclose information to the police, they can be confident about the level of safeguards.

I think it is a much better function to actually have every agency covered by privacy legislation, but to have exemptions built into the legislation for specific law enforcement functions. I think this is going to be even more of an embarrassment when we have national privacy legislation in Australia covering the private sector, because agencies like that are going to stand out as being in an anomalous position. My understanding of how data protection and privacy legislation works in other jurisdictions is that the police and intelligence agencies are usually in, but they would have fairly broad exemptions within that legislation.

CHAIR—Thank you very much indeed for coming. We are very much appreciative. Give our best wishes to Chris Puplick; he used to sit on this side of the table.

That concludes our hearing today. I would like to thank Dr Gaudin and other witnesses for their attendance. Thank you very much for having to put up with my rather poor sense of humour on occasions, and thank you to the staff. I declare the hearing closed.

Committee adjourned at 12.07 p.m.