PROOF VERSION ONLY

LAW REFORM COMMITTEE

Inquiry into powers of entry, search, seizure and questioning by authorised officers

Melbourne – 21 February 2002

Members

Mr R. H. Bowden
Ms D. G. Hadden
Mr P. A. Katsambanis
Mr T. Languiller
Ms A. L. McCall
Mr R. E. Stensholt
Mr M. H. Thompson

Chairman: Mr M. H. Thompson
Deputy Chairman: Ms D. G. Hadden

Staff

Executive Officer: Ms M. Mason
Research Officer: Ms K. Giles

Witness

Mr P. Chadwick, Privacy Commissioner.

Necessary corrections to be notified to executive officer of committee

The CHAIRMAN — On behalf of the committee I would like to welcome you to today's hearing. Should there be any matters you would like to speak to off the record we are happy to take evidence in camera or off the record. I draw your attention to the fact that once you get a copy of the transcript you are welcome to peruse it and return it to the executive staff. I invite you to speak to your paper.

Mr CHADWICK — Thank you for your initiative in this area with our office. It is a new office. I thought it would help if I sketched very briefly some background to that office, to give you a sense of the context in which Victoria has appointed its first Privacy Commissioner, with all that that might involve, for your reference.

The Information Privacy Act, as you know, was passed in December 2000 and took effect from 1 September 2001. It creates this office and it deals with information privacy not privacy, in the broad. Although I have authority under the act to address questions in public of privacy in the broad, the specific powers, et cetera, are confined to information privacy and I think that is significant.

Secondly, the objects of the act immediately require me and all of us who work under it to strike a balance between what is described as the public interest in the free flow of information and the public interest in privacy. So the Parliament has conceived this as a balance of two public interests and not as a clash between one public interest and variegated private interests. My functions include advice, research, education, investigation, conciliation and enforcement. The Parliament, recognising the thorough-going nature of a change like this — a law that deals with personal information in the public sector, which is really the molecules of public administration — the Parliament is giving the agencies a year to get ready and the enforceable powers under the complaints and compliance section of the law don't take effect until this coming 1 September.

The education function is a priority at the moment because Victorians are being introduced to 3 separate privacy regimes in 9 months. The one that I animate as commissioner, and I have just described; the Victorian Health Records Act which will deal with the privacy of health information after 1 July; and from 21 December last year, Victoria's private sector was covered by changes to the Federal Privacy Act. So 3 schemes, all dealing with different aspects of the privacy of Victorians. You can see the education task is partly disentangling those three and explaining to Victorians how it affects them.

Privacy is central to the issues being considered by this committee in this inquiry into the powers of entry, search seizure and questioning by authorised officers. For brevity's sake I will refer to all those relevant powers as "intrusion powers", just for the sake of convenience and brevity. There will be a written submission which details some of the points I will make. And because I am inclined to try to be practical, I have devised what I hope is a useful checklist for the committee. A checklist with particular reference to privacy, which may be laid like a transparency over any proposal to introduce a new intrusion power, or a proposal to renovate an old one, which is frequently the business of law reform, of course.

I begin with the purposes of privacy. I refer to a standard reference in this area, it is the book *Freedom in Australia* by Campbell and Whitmore, perhaps one of the earliest Australian books to look at this question and specifically to look at the powers of search and seizure. The authors say:

> The most that can be sought to be achieved within the complexities of the modern state is that the individual be left alone to pursue the good life in his or her own way where there is little or no impact on the common good of the community. Where the interests of the individual and the community collide, the latter claim must take precedence. Regard can still be had to the dignity and interests of the individual.

QUOTE NOT VERIFIED.

This quotation contains two of the fundamental notions in privacy. The individual has a right to be left alone unless the common good requires otherwise, and even where the common good does limit an individual's liberty, regard can still be had to his or her dignity. Privacy is a slice of the larger concept of liberty. Privacy is essential to the exercise of other aspects of liberty, including freedom of thought and conscience, freedom of expression and freedom of association. But privacy is also essential to the development of the self, to autonomy and to the dignity of the individual. So much for the theorists and the philosophers.

These are not trivial values. In balancing them against other values, as the act commands me, we need a sense of proportion. This is especially the case in the context of intrusion powers for authorised officers of the state because these abstract notions take practical form in that context. It is useful, especially in the context of your reference, to divide the privacy concept up into its different dimensions. This is commonly not done. First, privacy of the body. This dimension is critical to dignity and directly relevant to powers of arrest, power to strip search, for example, and power to take body samples. Now I know both of those are not technically within your terms because of

the way your terms exclude police powers, but I use them to illustrate the connection between privacy of the body — a dimension of privacy and intrusion powers.

Privacy of the home. The home is special in privacy law, and you will see references to it all the way through from the Universal Declaration of Human Rights in 1948. It is a sanctuary where we are free of the world's scrutiny, where we can relax the faces we wear in public and be ourselves. It is a place of intimacy and security. It reflects us through the ways we organise it and decorate it. We like to control who enters it and who communicates with us there. Powers for authorised officers of the state to enter and search the home override all of that, and the law has long recognised the significance of the intrusion and the importance of limiting the purpose and the exercise of those powers.

Privacy of personal belongings, again often neglected, is separate in privacy from privacy of the home. The sense of violation felt by all who have been burgled summarises sufficiently the significance for privacy of any state power that authorises strangers to sift through, examine and perhaps seize the personal belongings of others.

Privacy from surveillance. Not being spied on is perhaps the best understood dimension of privacy and certainly the popularly understood one. It helps to explain the disquiet, for example, about the increasing use of video surveillance cameras in public places. Again, that is not a matter for this inquiry, but a matter that helps to illustrate that dimension of privacy.

Privacy from eavesdropping. Technology permits now more than the traditional wire tap of affixed line telephone, use by the state of technology that constantly trawls through the tangle of wireless communication both voice and text, and can scan by key word and isolate particular conversations for attention is a higher tech form of search and seizure than we have been used to in the past. As communications change, as opening emails replaces opening envelopes, the same issues of liberty, privacy and the common good arise; the same disquiet is felt, the same presumptions apply.

Lastly, information privacy. In the e-world personal information is in some sense the person. Our details tell much about ourselves but never all, as anyone who has surveyed their credit card statements knows. Control over who knows what about us and for what purposes and to whom it is disclosed is the central concern of this dimension of privacy, the notion of control. When the state takes that control away from the individual, compels disclosure by law and authorises collection and use for purposes determined by others, it overturns the presumption of liberty in a potentially far-reaching way.

I go to that level of detail on the concept because I think it is the proper role of a specialised statutory office like this one to pay attention to the concept of privacy for a committee like this which is necessarily dealing with a very broad agenda and which is necessarily comprised of generalists on the issue of privacy. If my office can help, I think, in a constructive way, it is to give flesh to the notion of privacy for your committee. There are many others who will appear before you who will be able to deal with other concepts of liberty, et cetera.

I thought it would be useful to enter this topic and the privacy aspects of the topic by reference to some examples, if possible. I will not rehearse here the international standards that balance privacy rights and the need for the state to enter, search, seize and question. All I would say — and that is of course dealt with in my written submission — is that there is fresh significance in these international standards for Victoria because we have incorporated them in the Information Privacy Act. That is, these standards have a marvellous pedigree. We are not inventing the wheel with this new law, notwithstanding its recent passage. The standards we have incorporated are to be found in the major international standards and in most data protection and information privacy laws in the world. They, in their modern form, emerge from some 1980 guidelines of the OECD generated by a committee on which sat Michael Kirby, the then Chairman of the Australian Law Reform Commission. I lay emphasis on this and on the international standards because of the ubiquity of the technology. It is essential, I think, and I certainly have taken this to heart in trying the animate other aspects of my role — it is essential that Victoria look outwards and try for consistency in this area, since when we try to deal with information privacy we are also dealing with information technology, and it's ubiquitous and it does not know borders.

There are some specific issues from the committee's discussion paper that I thought it might be fruitful to examine. The first is the general issue of law enforcement agencies and information privacy, and by that term I mean law enforcement agencies defined under the information Privacy Act and it is quite a wide definition. Wide enough in some cases to encompass the bodies that must use the powers in your discussion paper's appendix listing different intrusion powers in the Victorian statute books in so far as you had located them at the time of that discussion paper, (and we have located a few more, included in that written submission for the purposes of trying to assist the

committee staff.)

A definition of law enforcement agency in the information privacy context includes agencies which are not primarily engaged in law enforcement that have some law enforcement function. For example, the Department of Human Services when it is dealing with child protection. But the section of the Information Privacy Act that exempts law enforcement is not a blanket exemption. It includes the requirement that the agency make a judgment that it is necessary for them not to comply with a relevant information principle, so there is a necessity test. There are also some enumerated purposes for which they can be exempt, it is not an exemption across the board. I lay stress on that partly because some agencies at the early stage of the life of the Information Privacy Act appear to misunderstand the Parliament's intention with that exemption, and I think it is important that I try to clarify that early.

The second reason I do it is that it forces us to reflect on the balancing between disclosure and discretion inherent in the Information Privacy Principles. If you are not exempt from the principles, then you are covered by them. If you are covered by them, how do they assist you when you are thinking of using an intrusion power or in your case thinking of legislating one or renovating an old one. Because those principles contain much of the best international thinking in this field and because Victoria has intentionally chosen that broad international standard, there is a lot of guidance for how you do the balancing. For example, in IPP2, Information Privacy Principle 2, which deals with use and disclosure of personal information, there are some defined exceptions, as you would expect they cover things like public health, investigation, detection of crime and those sorts of things. So I encourage the committee and others who might read the transcript and think through these issues because they have an intrusion power to use, to look to the Information Privacy Principles as a consistent and common standard. Otherwise, we will distort the law of Victoria by building into various statutes many exemptions from the overall privacy balancing tool that you've enacted in 2000, the Information Privacy Act. You would have seen that before. I certainly saw that after the passage of the Freedom of Information Act, where agencies would attempt to have exemptions put by the Parliament into other legislation. The effect of which was to second-guess the Parliament's overall judgment about the balance between, in that case, openness in government and appropriate secrecy. I foresee the same possibilities here, and essentially when you have such a wide range of legislation before you, I think the point is worth making here.

A very practical and in many ways sensible example of the powers to question, one subset of what you are looking at, it is the example of seeking the names and addresses of public transport users. You would be aware that the public transport operators are at present in Melbourne undertaking what is typically termed in the media a "fare evasion blitz" . The powers they rely on is one of the Powers referred to in your discussion paper and it is a matter that has come before me as well in my early months of my office. I propose to step through very briefly the key issues. Just the key points — details in the written submission, the staff deal with some of it in your discussion paper. — But I think it highlights something important because it takes the issue of intrusion powers away from what might one might call the serious, very criminal type of context that we are traditionally dealing with — search warrants, telephone taps, et cetera — and it puts it into the ordinary lived experience of thousands of ordinary Victorians. And I suspect that is an important issue for you in weighing up this area. It is an accident of fate that we have such a live example of such an every day power to question before us at present.

The Transport Act 1983 appears to contemplate travelling on public transport without a valid ticket. It says explicitly that that is lawful if: the person took all reasonable steps to get the ticket before beginning the journey; had a reasonable opportunity to buy a ticket during the journey; and took all reasonable steps at the end of the journey. That is the first and key issue. When is a person travelling lawfully without a valid ticket? Many of the answers to these questions are not properly the business of the Privacy Commissioner or of this inquiry. They are decisions for others. But I go through them for a reason. When a person hops off the train at Flinders Street and approaches the barrier and finds the ticket inspectors a conversation begins. If on their way to work they tried to get a ticket from the machine but it wasn't working, and because they were worried about being late for work they jumped on; and didn't walk, say, 10 minutes to the milk bar to get a ticket. The first question in law is whether they took all reasonable steps to get one before the journey. I will return to that.

Typically there is not an opportunity to buy a ticket on the train or tram because there are no conductors or machines that sell tickets on the trains — different for trams. When they get to the barrier, the ticket box to buy the ticket is now on the other side of the inspectors, so a question arises: Under the Transport Act what does the authorised person have to believe before he or she can exercise the power to request name and address? The act says they have to believe on reasonable grounds that an offence has been committed or is to be committed. What constitutes reasonable grounds in the context of Melbourne's public transport system at present? I won't rehearse the detail. It is clear that there are some difficulties with the ticket machines. The details needn't delay us. An

important question is what the inspector must believe on reasonable grounds in order to then exercise the power to question. That issue arose in the first blitz last year. It is now common ground, I think, that it is not reasonable grounds just to have the person say: "The ticket machine wasn't working at my home station". Say it is Frankston, it could be anywhere.

Ms McCALL — Constantly Frankston!

Mr CHADWICK — Okay, it could be anywhere, and I am sure there is plenty of work being done on it. But for my purposes it is just whether that constitutes "reasonable grounds". It seems to be common ground that it doesn't. The private transport operators have now established a system, I am advised, whereby they seek an electronic check of the machines to see if they are working, basically overnight, but it is a continuing process. And they give a list of the machines that are not working to the inspectors. The procedure at present is that the inspector will look at that and see if the passenger's home station is on the list. If it is, the passenger walks through to get a ticket and there is no further drama and certainly no exercise of the power, which is what we are concerned with.

If it is not on the list, I am advised that it is possible for the inspectors to make a mobile phone call to check whether or not that list has been updated since the remote check was done in the small hours of the morning. If the answer is still that that location is not on the list, then the person will be asked for his or her name and address.

All I wish to say at this point about that is that you can see that the power is being exercised in a changed circumstance from when the power was created. The power predates privatisation. It predates the removal of conductors and station staff who sell at a ticket window. I leave that for the committee's consideration: It is not properly the business of the Privacy Commissioner until someone comes, if they do, to say someone has collected the information about me, my name and address, unlawfully, because information privacy principle 1 says that you can only collect information necessary to your functions and only where that is lawful, fair and not unreasonably intrusive. It may well be fair and not unreasonably intrusive. It is a conversation, hopefully courteously conducted at the barrier of the station, but the lawfulness of it is a matter for me because of the information privacy principle 1. The lawfulness of it requires me to look at that section of the Transport Act — something which is also before you.

The next stage, still with transport, is that the authorised persons have the power to detain for arrest. The privacy of the body is implicated. Dignity is implicated. There are serious issues here. The power to detain might be exercised where the person does not give name and address or the inspector reasonably believes that they have given a false name and address which takes us to the issue of verifying information. It is common practice, I am advised, that when someone gives a name and address the inspector would ask, 'Can I have a look at your driver's licence, have you got a gas bill on you, bank statement, something that will tell us that you really are the person you've said you are?' There is a distinction here between sighting that document and copying or recording the details of it, because for privacy purposes you ask yourself whether that is necessary for the function. In any event, my staff and I can find nowhere in the Transport Act that authorises the person to seek the verifying details. If as a matter of public policy the Parliament concludes that that particular power to request name and address, in order to work in practice, needs some verifying detail, then some attention, I suspect, needs to be paid to whether or not the power exists to do so. We have looked for cases on it. There appear to be none. I have sought advice from the relevant officers of the Department of Infrastructure: There appears to be no law on it and I suspect it is an issue because of the practical nature of it for your constituents.

Can I move now to the issue of audio or video recording of entry and search. It is suggested — —

Ms McCALL — Can I jump in? You and I may seek to differ on a number of these issues, but that's okay. The question on when it is appropriate to ask someone about their name or address or intrusion into their personal belongs, two particular issues, one is when you shop at Ikea when you pay they always ask for your post code, where you live. The second question is the right of a department store to search any shopping bags that you may actually take into the department store before you've actually shopped there. Now those two, in my mind, sort of come under what you are trying to say. Do you consider those to be intrusive?

Mr CHADWICK — Can I make a couple of distinctions. I am not trying to make a generic point.

Ms McCALL — You are the Privacy Commissioner.

Mr CHADWICK — Sure. Let me be clear and leave aside the question I am trying to isolate for the committee, which is that you have to look at that as particular to the Information Privacy Act, and I am trying to highlight some issues that have come across my desk. The two examples you've raised, thinking about them in

pure privacy terms, the first one you would ask is the post code per se personal information. The definition is information that would allow a person's identity to be readily ascertainable. You've already got the name and address, what does the postcode add?

Ms McCALL — Ikea don't; they get your name if you buy by credit card. Yes, that is accessible; they could search you on the electoral role.

Mr CHADWICK — That is why I qualify my answer. That is a very different question. I know it is before you as parliamentarians in Victoria, but the question of access to the electoral roll or to public registers is a very live issue for my office and for me. Can I leave that for a moment and come to the shopping bag point. On that point I suspect it is a matter of consent. The request is put by the check out person, 'Do you mind if I have a look in your bag?' And what hangs in the air is — —

Ms McCALL — 'Can I say no?' And I have done, interestingly. It is very interesting to watch.

Mr CHADWICK — Was any lawful power referred to when you said no?

Ms McCALL — The manager appeared.

Mr CHADWICK — Was it resolved in the sense that you were operating under the law?

Ms McCALL — The issue is who has the authority and that is really what I am trying to get to and the issue of intrusion.

Ms MASON — Many shops have a sign so you are giving consent when you are entering the shop.

Ms McCALL — But they do it on your way in.

Mr CHADWICK — Can I ask is there a state power here, some retail legislation or something?

Ms McCALL — It is not under the Retail Traders Act, no.

Mr CHADWICK — It may be that they have advice that it comes from some old mercantile corner of the law about some sort of reason.

Ms McCALL — I digress but they are issues that come to the fringe of what we are talking about.

Mr CHADWICK — All I say by way of trying to assist is that when they involve a private sector setting like Ikea (or any retailer, I don't mean to isolate that example) or any other private sector setting, you will find that the National Privacy Principles are very, very similar to the Victorian Information Privacy Principles, partly because in 1996–1997 when Victoria was considering what was then called the Data Protection Bill, our principles were very influential in the creation of the federal national privacy principles. It is significant, I think, that on this issue the parliaments that have so far addressed it have addressed it in almost a bipartisan fashion. Certainly a fashion where opposition was not put to the fundamental principles that both those parliaments were enacting. I don't want to detain you, please stop me if you want me to stop, but on the separate and isolated question of public registers I should explain further. The Parliament of Victoria, I think, rather wisely, did not try to develop a detailed mechanism in the Information Privacy Act to resolve the many issues that arise in relation to public registers and privacy. It said instead that anyone with responsibility to administer a public register should do so consistently with the information privacy principles so far as is practicable. The Parliament then left it to those administering authorities and to the Privacy Commissioner to work out what that means in all the many particular cases.

The public register that I think is unique and requires unique thinking — and therefore shows the wisdom of Parliament's judgment, in my view that there is no universal fix for this issue of public registers, they are all different and have different rationales —is the electoral roll. It has a very important democratic purpose but it is also rich in the personal data of Victorians in an age when the computer assists the gathering, collation, assessment, copying of personal information for non-public purposes such as direct mailing, et cetera, customer profiling. One of the issues on which I have had some discussion with the Electoral Commissioner in an informal sense is this issue, which I am sure the Parliament will address, of the proper uses of something as significant to a democratic community as its electoral roll: Weighing up that question of disclosure on the one hand and discretion and privacy protection on the other. Unless you would like me to pursue in any greater detail the question of public registers I will leave it there.

The CHAIRMAN — I would be keen, just before the questions, we were about to move on to videotaping and if you could provide some comments about that.

Mr CHADWICK — The comments I have now are quite brief. On the question of audio and video recording, it is suggested in the discussion paper that that might be an habitual process because it creates a safeguard to make sure that the exercise of the power of entry, search or seizure was exercised properly by those who are charged with that duty. But from a privacy point of view, quite important issues arise when you video or audio tape an event like that. I want to use strip searches because the example is so vivid, but as I have said earlier, I recognise that they are not within your terms of reference because I understand that — please correct me if I am wrong — that your terms of reference try to distinguish those powers exercised only by police.

The reason I raise strip searches is that there is nothing more privacy invasive than a strip search conducted under force of law by agents of the state. It has entry, search and, especially if a body is taken for DNA database purposes, seizure. It has entry, search and seizure implications all in one. It implicates to a very large extent dignity, a core privacy notion. If you add to that for the person subjected to the search the knowledge that the camera's eye is watching and recording and that the episode will be forever remembered in a digital form, you create a worse suffering from a privacy analysis point of view. You create a greater indignity even though your public purpose, your initial motive, is a sensible one to create that kind of, as it were, objective record of the exercise of the power.

Without expressing a concluded view, one of the things that I would urge on the committee is consideration of whether or not video recording and audio recording ought to be something that is encouraged across the board because there will be many contexts in which to video the use of an intrusion power, will implicate not only the dignity of the individual but the privacy of others. For example, the exercise of a power to enter a farm where, say, there might be some concern about an animal disease, there might be other people on the farm reacting in a certain way. People will be conscious of the possible impact on their neighbours. The presence of the inspectors might be a very unusual experience for the people going through it. And the presence of someone with a video recording adds to that distress.

From there we move to what happens to the record. It is not unknown for some of these videos to emerge in the media. Of course it is improper, but it has happened and those sorts of issues need to be considered as well as other things that one traditionally asks in a privacy context. Can copies be made? Who is allowed access? Can the copy be retained? What is a Public Records Act type of requirement? That sort of thing.

One of the key issues in information privacy is that if you don't collect it, you won't have dramas up the track, with use, disclosure, storage, retention. So the question especially for the Parliament, (leave aside the administrators and their discretions) is should this be collected? What is the need? And does the need outweigh the reasonably foreseeable costs in privacy, (among other things, which others will address you on).

Moving on to D under subsection 4 of the outline to the written submission, there is a suggestion that data might be aggregated and a report made about the use of all the many different intrusion powers. Naturally I would support very strongly the accountability that is inherent in that. But I would raise a couple of questions from a specialist privacy point of view. And they are not objections, they are not questions of principle. They are questions about how well we tailor a procedure like that if you wanted to mandate it. If you aggregate sensitive data in its raw and identified form, you increase the chance that the leak will do irretrievable privacy damage. It is better, on the whole, to disaggregate sensitive private material and hold it in many different places not in one. So if the proposal is to create a reporting requirement, I would urge that the committee consider whether the reporting be of de-identified information only, for example, statistical information or de-identified case studies. And there is plenty of learning of course on how that is achieved.

Hopefully that will allow the proper balance to be struck between transparency and accountability on the one hand and privacy on the other in areas where the exercise of these powers is sometimes serious in relation to privacy, not just of the person that is targeted, but of third parties who are not targeted, who are innocent third parties. One example, to revert to the public transport scene, is that where an inspector seeks verifying information and someone does not have any document on them or they are young, the inspector might ask for mum or dad's mobile and name and address. So immediately there is a collection of personal information about a third person who is not themselves suspected of any offence. That is the only point I make from a privacy point of view, because you start from the point of view, well, is it personal information, has it been collected, and then you look to need. As I have said, if there is an issue there with that aspect of the Transport Act it is something the Parliament can step through knowing that it has established general standards for the handling of information privacy, rather than the

establishment of all sorts of different mechanisms to do that.

Can I finish with a privacy checklist, how to be most practical about this. I presume there will be many tests against which you have to assess a proposed intrusion power or the reform of an existing one. Privacy is only one of them. And you've listed the Senate committee's generic tests. Where an existing or proposed power to enter, search, seize or question is under consideration it should be assessed for its privacy impact, and here I am speaking only about privacy impact, against the following questions: How does the power affect privacy in any of its several dimensions? Privacy of the body, privacy of the home, privacy of personal belongings, privacy from surveillance and privacy from eavesdropping. That enforced disaggregation of the different dimensions of privacy can assist in an analysis that has to be made when considering an intrusion power.

The second question: What is the public interest to be served by empowering authorised officers to use the power, and is that public interest sufficient to override an individual's right to privacy in every circumstance? If not, how should the power be qualified to ensure privacy rights can prevail in certain circumstances? The balancing is inherently, required by most privacy legislation, but in this checklist, the balancing is forced upon the decision-maker. Is the power precisely limited to that which is necessary in the circumstances to achieve the stated purpose? In privacy, purpose governs use. It is absolutely essential that purpose be clearly defined.

Will the procedures for the use of the power be proportionate and any intrusion into any individual's affairs be kept to a minimum, especially for uninvolved third parties? Have all the less privacy invasive procedures been adequately considered and found wanting? Is there a need for independent authorisation to use the power so that those who want to use it are separated from the judgement that it is necessary to use it? And here by analogy we have the warrant process for telephone taps. A *want* to use it, but a different judge of whether it is *necessary* that the power be used. I can't make a specific comment about every different provision you are looking at, but it is the kind of generic test you ask in privacy terms.

Are the persons exercising the power expressly accountable for unauthorised privacy breaches? What I mean by that is are the persons who exercise the power accountable expressly for unauthorised privacy breaches? So you can have an accountability mechanism, but does it include the criterion: Did they invade privacy in an unauthorised way? That sort of thing. It turns the mind of those who are applying the accountability mechanism to the activity in relation to privacy as well as activity in relation to something else, like theft of the material or something that might also be improper.

Has Parliament considered what happens after the power has been used so that the impact on the privacy of the individual concerned and any third parties is minimised? For example, who will have access to the information collected? How will the information be stored? In what circumstances will the information be permitted to be used or copied or retained? The notion of copying is absolutely critical in a digital environment. It mattered far less in a paper environment but one must always have this in mind nowadays. The recent Transurban example of credit card numbers is a good example to illustrate that point. It is so easy, so swiftly and so widely to replicate digital data. In what circumstances will the information be permitted to be used or copied or retained? Who will determine when it is appropriate to destroy personal information or return property after the public purpose has been fulfilled?

Last on the checklist: Is the process as transparent as the circumstances permit? For example, at a minimum, is there provision for independent audit similar to the way the Ombudsman audits telephone tapping in Victoria, and audits use of data for enforcement purposes out of Citylink? Is there independent audit and provision for public disclosure in de— identified form of statistics about the frequency of use of the power. Just the bald statistic might, when reported through the Parliament, be an appropriate check, if there were a year when the use rose very steeply. It would be a warning signal to the accountability authorities and to the Parliament itself that perhaps that power has become rather too frequently used given the way the Parliament tried to constrain it.

Thank you for your attention, and I will try to answer any of your questions.

The CHAIRMAN — Thank you, Paul.

Mr BOWDEN — Paul, I have a question which may be of interest. Your media release about passengers without tickets and privacy rights and so forth, as an ex-journalist how do you reconcile the public's right to know versus privacy? I will just paint a little picture here. Paul Chadwick hops on a train in good faith, the machine doesn't work at the station. Paul Chadwick hops off at Flinders Street and hasn't got a ticket, the inspectors are there and you have a brief discussion with the inspectors. However, being a Privacy Commissioner, a journalist adjourn list happened to be at Flinders Street Station and sees you talk to go the inspectors so next morning we all open our papers and there is a beautiful smiling picture of you and says, Privacy Commissioner Quizzed on

Fare Evasion' — a straight-out invasion of your privacy and a false accusation. And you have a public office, we have public office and I think at times the journalists really cross over a very, very important line.

My question is: As an ex-journalist and through your present responsibility how do you reconcile the public's right to privacy?

Mr CHADWICK — I have to wear it. It happened in a public environment. The exchange was over heard. The journo reported it about me; as someone who holds a public office I have to wear, like you, a greater level of scrutiny and it will include that kind of scrutiny. Whether, though, the story is accurate is a quite separate question. What I am saying is that I am fair game for the journalist to do that. That is my view.

Mr BOWDEN — As the Privacy Commissioner, do you have a view on the desirability of that?

Mr CHADWICK — I will return to that. That is one part of the question: Is it within the compass, as it were, of freedom of the press to report that? My answer is, yes. But the freedom of the press brings something else. It brings a duty to try to get it right, to try to get it accurate. For example, to offer the right of reply, so that the journo, instead of just quietly listening to this exchange, bales me up afterwards and says, 'What do you think about that, you are the Privacy Commissioner?'. And there is a chance for me, as there ought be for anyone, including you, who are subject to media questioning and attack, to make a reasoned reply which is then reported fairly and accurately.

Ms McCALL — Great in principle, doesn't happen in practice. That is double standards from where I sit.

Ms HADDEN — If it is reported accurately, that is the other issue.

Mr CHADWICK — Can I ask whether you mean the media are exercising double standards or I am in that answer?

Ms McCALL — I think the media and if they should be exempt from some of the things you are talking about is a gross misuse of their power.

Mr CHADWICK — The question involved the large issue of appropriate limits of freedom of expression versus rights to privacy, an issue I had to deal with both as a practising journalist and when I served on the committee chaired by Frank Brennan and others where we looked at the journalists' code of ethics and we had to think about privacy issues, especially privacy of public figures. I have published on this issue and if the committee is interested I will organise for those papers to reach you.

On the broader question, the norm in journalism ethics is where something is obviously private but about a public figure, at least two tests have to be applied: What is the public interest as distinct from public curiosity or public prurience, or whatever it is. What is the public interest in disclosing those private facts about that public figure? The classic example that is usually given, at least in theoretical terms and usually in the American context of media journalism and ethics, is where the President might be suffering from an illness that could seriously impair his or her judgment. The journalist will say that in the absence of disclosure of the President's impairment, that there is a public interest overriding the President's privacy interest in disclosure of the President's ailment. That's the argument. That's the rationale. Now of course there are varying degrees. One obvious one is the financial affairs of a public figure. One ought to be able to show, in order to justify disclosure in the media of the private financial affairs of a public figure, a nexus between those particular financial affairs and his or her public duties. What I am rehearsing for you is the standard analysis that one would make in receiving private information about a public figure and doing the balancing which not the law but media ethics requires in this case, because as you know we haven't covered media with privacy law in that way.

The High Court addressed aspects of this in the case of the *ABC v. Lenah Game Meats* last year. I don't have the citation. I can get it for the record, but it addressed aspects of this question of media, privacy and, in fact, technology. It is a rich area and I am sure perhaps one day we will discuss it in more detail. As a former journalist all I can say is that any proper understanding of the freedom of the press means a proper and serious analysis of what your responsibilities are as well.

The CHAIRMAN — Thank you, Paul. Our time has moved on. We allocated 45 minutes which we have fulfilled for your time, Paul. I am conscious some of my colleagues may have some lunchtime commitments. We need to get some answers to some final questions.

Mr LANGUILLER — Thank you for your excellent contribution. I think you answered as many

questions as you've generated for this committee, so I thank you for that. There are a couple of questions I wish to put to you. You referred to your office's role in terms of education; could you elaborate or submit to us at a later stage what you do in relation to non-English speaking-background people? I think there is particularly a special chapter that ought to be devoted to young people, minors, youth and so on, and people with disabilities. In addition, if I may, which is a very broad question, but 11 September I think has changed our lives as we discovered in our recent travels and I wondered if you may have any brief, succinct comments you may wish to make with respect to the way in which that may impact on our community. For those of us who have recently been overseas — and I was going to ask you if you have recently been overseas — you might have noticed how much of our bodies so to say are inspected, and issues that you raised before certainly were brought to our direct experience.

Mr CHADWICK — On non-English-speaking people I am acutely conscious of the make up of the Victorian community that I serve, as you do. I have attempted to get the basic information brochure translated into the major languages and out at this early stage, and more will follow. On minors, absolutely, there are two aspects there: One is how we bring young people to an awareness of respect of privacy, because on the whole young people don't have much privacy. The sensitivity for privacy grows with once maturity and, the cynic would say, one's "store of secrets" grow. And I mean that, of course, facetiously. The sensitivity to privacy and the awareness as to why it matters as a subset of liberty is usually something that comes with years. That is not to say that young people don't have the instinctive wish for privacy and all of us with adolescents will recall some of the ways the developing young person reaching toward adulthood starts to assert his or her selfhood and individuality partly by making demands for privacy. — Physical, within the household, shutting bedroom doors, and all of that. And also information privacy about his or her diary or laptop, or whatever it is nowadays. So on the issue of minors, there is that question, what does one do, as an educational challenge to bring the Victorian community to that awareness in that age group, because they are the adults of tomorrow. They are the ones who have such a facility for this technology which has such a fantastic capacity to augment government, public administration and commerce and if misused, to invade privacy.

On 11 September, I made an speech on this point and I will send a copy. Very succinctly, clearly 11 September requires all with public responsibilities to think about the proper balance between liberty and security. Without rehearsing all the stuff about privacy being a subset of liberty, it implicates privacy very much. I would say no more than this: There are three tests which I think can sensibly be applied when any proposal to reduce liberty is put forward nowadays in the wake of 11 September. The first test is a proper process should be followed in a proper and timely way. You will all probably know the great story about Thomas Jefferson being asked why he had proposed for the American system the Senate as well as the House, and he held up by the saucer a cup of tea he was drinking, saying, 'That stops me burning my fingers on the cup'. It is this idea that we have created institutions, including the one you now serve, that has built into it checks to stop haste in law making. It is I think, one to remember nowadays in the wake of 11 September. On the whole Australia seems to have taken that to heart.

One very salutary story is of the enactment of section 2 of the Official Secrets Act in England in 1910 on the back of some sort of scare to do with the navy. Media hysteria, all the rest, and the passage of section 2 of the Official Secrets Act occurred in 50 minutes. The minister with responsibility for it couldn't believe it and the parliamentarians who got to their feet to ask the obvious questions about the balance between liberty and security in their day, in their Parliament, were physically pulled back to their benches according to the minister who proposed the measure. There are lessons from history about hasty law making bad law. That is the first check.

The second check is judicial oversight. We are all familiar with that from all sorts of contexts especially, for example, telephone tapping. Let's build judicial oversight into any measures that infringe liberty in the name of security, because the Executive can, we know from experience, get things wrong and sometimes judicial oversight is appropriate.

The third check is that there be as much transparency as possible in the administration of those sorts of measures as well. If you are interested, as a committee or even individual members, I will make sure I send a copy of the paper that tries to bring these issues to a succinct form.

The CHAIRMAN — Thank you, Paul.

Ms GILES — I have a very quick question, a point of clarification. You may have covered this in your written submission so tell us if it is covered. You mentioned a checklist for agencies. What form do you think that checklist should take? For example, I know that your office has the power to approve codes of practice. Do you think the checklist should be in the form of some sort of code of practice or do you have any ideas about

implementation of the checklist in practice?

Mr CHADWICK — I would look at the code-making aspects of the act, but intuitively I would say no because what I have proposed here is a check list for creating a sieve that a parliamentarian might put a proposal through in order to see what the effect on privacy might be, that's all. I am sure others would sit before this committee, as have others who deal with civil liberties or something else. All I am saying is that if you want to try to establish the proper balance between privacy and an intrusion power, it is useful if the lawmaker asks himself or herself those questions in the check list.

Ms GILES — What about the agencies themselves? Is there some sort of recommendation?

Mr CHADWICK — I think many of the checks I have proposed for the lawmaker would in a different form be applicable and useful when you come to the detail of your report and recommendations. I hope so, anyway.

The CHAIRMAN — My colleagues have some questions.

Mr STENSHOLT — You mentioned a checklist, et cetera, but of course you've got many, many laws and regulations where they handle, for example, name and addresses —the one you raised. For example, it has to be reasonable, or another one says where an offence is being committed, another one says where it is likely to be committed, another one says that the officer has to give their name and place and give it in writing if necessary, and another one meets that completely. Other ones say they have to explain what they have to do. Other acts omit that type of thing completely. I know why you have beliefs and principles, but the issue of some kind of consistency between various acts, would you have a view on that? It would help us.

Mr CHADWICK — I would endorse consistency for the reasons I tried to show, because consistency in privacy standards is so important: the technology; the similarity of different jurisdictions; the international pedigree; and therefore the learning and experience. Consistency is important. As a matter of statutory elegance it is not a good idea to put all these privacy laws in different statutes, including exemptions, where you already have a standard where minds have applied themselves. So, on the consistency point about what these intrusion powers should extract from the citizen, all I would say there is that I suspect — I am guessing — that, like the public registers point, you will find different public policy rationales for the different powers, and when you come to address it I suspect that only you will be able to hazard that kind of generic test: What comes with name and address? I have tried to highlight it for the public transport system currently to do this proper enforcement task, which is an important task. I don't want to be misunderstand stood as suggesting that somehow the right to privacy trumps paying your fare. You've got to pay your fare. That's important. But in the many areas of the statute book where these powers arise, and in the very broad spread of contexts that your staff showed in the discussion paper and we had a look at, it seems to me you are going to need some pretty broad generic tests as to why we extract more than name and address but also you will be thinking: "Once we have extracted it for that purpose, what are we doing to try to stop its use for other unrelated purposes?"

Mr STENSHOLT — That is usually left out.

Mr CHADWICK — Exactly and I am suggesting the information privacy principles are the generic standard and if you were perhaps establishing new powers in different statutes they might have reference to those standards, import them and in that way we develop a coherent law of privacy.

The CHAIRMAN — Eloquently expressed, Paul, thank you. We will now adjourn for lunch.

The witness withdrew.