

TRANSCRIPT

ROAD SAFETY COMMITTEE

Inquiry into serious injury

Melbourne — 28 October 2013

Members

Mr A. Elsbury

Mr T. Languiller

Mr J. Perera

Mr M. Thompson

Mr B. Tilley

Chair: Mr M. Thompson

Deputy Chair: Mr T. Languiller

Staff

Executive Officer: Ms Y. Simmonds

Research Officer: Mr J. Aliferis

Witness

Mr D. Watts, Acting Privacy Commissioner and Victorian Commissioner for Law Enforcement Data Security, Privacy Victoria.

The CHAIR — Mr Watts, on behalf of the Victorian Parliament's Road Safety Committee it is my privilege to welcome you here today to give evidence in relation to our inquiry into serious injury. By way of background, evidence that is given is protected by parliamentary privilege. Comments made outside the hearing are not afforded such privilege. The transcript will become a matter of public record. Should you wish to give any in camera evidence, we can move into an in camera setting. You will receive a copy of the Hansard transcript of your commentary today. You are invited to make any necessary corrections to typographical or factual errors and return it to us, at which time we will put it on our website.

In starting, it would be helpful if you could state your name and position. I now invite you to commence with those details, followed by your presentation.

Mr WATTS — Thank you, Chair. I am David Watts. I am the Acting Privacy Commissioner. For the last five years I have also been the commissioner for law enforcement Data Security. Those are positions I hold concurrently. If you are not aware of what the Commissioner for Law Enforcement Data Security does, I regulate the security of Victoria Police's law enforcement data. That raises some security issues, which might touch on some of the things that we need to speak about today. I am very happy to touch on those if that is what is required.

The CHAIR — Thank you. Would you like to speak to your presentation?

Mr WATTS — I have distributed to the members of the committee a short document. What I have tried to do is give you not the answers to all of your questions but a road map of what some of the relevant issues might be and how some of them should be approached. I had meant to have that with you before now; my apologies that I was not able to do that. I will refer to some of the points that are made in this document. I have attempted not only to simplify things but also to give you some of the major concepts that are relevant to your considerations, as I understand it.

I will start by thanking you for inviting me to participate. The information issues the committee is grappling with are of great public importance, but they are of some complexity too, so I thank you for inviting me to comment on them. I also want to thank the committee's executive officer for having sent me a very informative and useful document. I am at a disadvantage a little, because I have not heard all of the evidence that you have heard and have not gone through all of the transcripts. I do have a document from the executive which raises a number of different questions, and I am happy to go to those and speak to them in detail.

I will make a couple of fundamental points. The Victorian Information Privacy Act is a default regime that governs the collection, use, disclosure and other handling of personal information in Victoria in the public sector, except to the extent where it is inconsistent with other legislation. That is a really important point that is often overlooked in information and privacy debates.

The second point is a related one — that is, that privacy is just one component of the information law landscape. There are lots of other laws that relate to information and restrict the ways in which institutions, whether private sector or public sector, deal with it. They range from intellectual property law, through to secrecy provisions, through to confidentiality obligations and through to specific statutory provisions that relate to or that authorise the provision of information or restrict it.

I also want to touch on criticisms of privacy, because I am sure you have heard some of those during the course of your hearings. There are a number of criticisms of privacy: that it inhibits the appropriate sharing of personal information, impedes efficient service delivery and discourages technical or technological innovation. I would argue that on some occasions that is correct, but on most occasions it is not. You actually have to search for the solutions in quite complex areas of the crossover of regulation. Again, I will come to that in a moment.

Paragraph 5 of the section deals with sharing of personal information and basically sets out the tools that are available from within the privacy act. It notes that IPP2.1 — by the way, the IPPs are attached to the briefing for your convenience — permits the disclosure of personal information for the purposes of research or the compilation or analysis of statistics in the public interest other than for generally available publications. It also notes that law enforcement agencies such as Victoria Police are substantially exempt from the restrictions on the use and disclosure of personal information.

I have put a final paragraph in — paragraph 6 — related to data linkage, which as I understand it is an issue that has been raised before you and which has become quite complex.

I thought I would add attachment 2 to the paper just to give you some general background. It is taken from the Population Health Research Network and is a description in general detail about what data linkage is. From that page there is a whole range of supporting documentation that the committee might find of use in looking at and trying to understand what data linkage is.

Data linkage is a technique that predominantly tries to do two things. It tries to ensure that the sharing, for want of a better word, of various datasets of personal information does not constitute personal information — or health information, for that matter — and therefore the legislation does not apply to it. It de-identifies them or anonymises them. There is a whole range of terminology that covers that particular technique, but it attempts to ensure that the various aspects of the datasets that are to be shared do not constitute health information or personal information and therefore are not felt to cover or be covered by privacy legislation.

There is a cognate issue — that is, an issue of legal authority. The significance of that issue is that if you are collecting and wanting to share a whole range of disparate datasets, you need the legal authority to do it in the first place. If you have a very narrow remit, it is very difficult to share datasets that are outside that remit. Questions of legal authority loom large in the sort of analysis that is in front of the committee, and looking at issues of legal authority, and what you are entitled to do as an agency and what various agencies can do under each of their charters and each of their sets of legal authorities is also really important.

That is very much a Cook's tour of the briefing that I have given you. I also make this point: privacy is not an absolute right. It is an important public interest, but there are other important public interests. The legislation recognises that in two ways. Firstly, it is recognised in its objects clause, saying that it is designed to promote the free flow of information whilst at the same time protecting people's expectations of privacy. What is often overlooked is the fact that one of its objects is to promote the free flow of information. Within the information privacy principles, which are in attachment 1, IPP2 is the provision that deals with the sharing of information and the use and disclosure of information.

Perhaps I will finish at this point. I know you have lots of questions. If you want me to go on, I will, but I will take guidance from you, Chair.

The CHAIR — Thank you for your brief overview and for the scholarly paper you submitted to the inquiry, which we greatly appreciate. I would like to start with questions. Feel free to incorporate some of your material in responding to the questions. That might be a good way to move forward.

Mr WATTS — If it is worthwhile, I should say something that I said to you earlier, Mr Chair, and that is that some of these issues fall within the jurisdiction of the health services commissioner, who administers the Health Records Act, which deals with health privacy. The Information Privacy Act, which I administer, does not cover health information. I am very happy to provide you with guidance in relation to health privacy issues, but there may be issues of detail that I just simply cannot get to or at least cannot answer positively today. That might be a matter for the health services commissioner, or it might be a matter for me to come back to you with, whichever is most convenient for the committee.

The CHAIR — Thank you very much. I would like to ask my colleague Mr Languiller to commence with a series of questions.

Mr LANGUILLER — Thank you, Mr Watts, for your submission and your very good presentation. Can I call you David?

Mr WATTS — You certainly can.

Mr LANGUILLER — We will need to go through the motions, as you might appreciate. During our July public hearings Peter Carver from the Department of Health responded to a question about how the disclosure aspects of the Health Records Act 2001 might affect the collection and linking of road crash injury by saying the following — I am happy to repeat the long sentence to provide clarity if you wish me to. Peter said:

We are able to do it under the Health Records Act, providing it is within the purpose of the objectives of the Health Services Act. We have consulted with both the privacy commissioner and the health services commissioner, and they are in agreement with what

we are doing. The health services commissioner releases a set of guidelines around what can be done in terms of individual health records. They are prepared to look at that should we require it. We are also taking further legal advice about whether or not to improve the protections we need to establish a statutory function within the Health Records Act or the Health Services Act that carves out data linkage as a specific statutory function with defined responsibilities. That is a work in progress.

That is a quote. Does that mean that data linkage, where data from Victoria Police, VicRoads and hospitals is combined, could only comply with the requirements of the health records and health services acts if it was undertaken by the Department of Health and not by another government entity such as VicRoads?

Mr WATTS — The answer to your question goes back to the point I made initially, and it is this: the wrong way to start analysing privacy is to look at the Privacy Act, strangely enough. The correct way to do it is to actually look at what your legal authority is. What are your powers? What are you permitted to do? If you look at the legal landscape that applies in this complex area, you have health-related legislation, like the Health Records Act. The Health Services Act is one piece key piece of legislation. Within the Health Services Act there are some very strong confidentiality provisions. From memory — and I say that in bold italics — it is section 141 of the Health Records Act. That very much restricts what health information can and cannot be released by people who work within the department and in health services.

The way I interpret what Peter said to you — and I know Peter well and have worked with him in the past — is that he is actually going back and affirming what I am saying to you: that there are questions of legal authority. ‘Do I have the authority to collect all of this information?’ is the initial question that anyone has to ask in this complex area. ‘What do the statutes say? What are my legal powers? What are the restrictions around that?’. If I am correct in my recollection, section 141 is one of the restrictions that the Department of Health would look at.

There are other confidentiality obligations arising out of other general government legislation, the Health Records Act et cetera. It depends on exactly what the dataset is. It is difficult for me to tell you all of the pieces of legislation that would be relevant in the abstract. But what Peter is saying is absolutely correct: let us look at what our statutory functions are.

Once you look at the statutory functions and determine how broadly they are fairly interpreted, then if the answer is that we do not have enough power to do what we are looking to do, or to do what we want to do, then you are looking at some form of legislative amendment to permit you to do it and give you that power. I understand that there is now a data linkage unit within the Department of Health and that Peter leads that unit. When Peter says that those things are works in progress, I think that is what he is saying — that they are looking at what the extent of their legal authority is in order to be able to determine whether what they do is authorised by law because they do not want to step outside the law. In general I would agree with what Peter is saying.

Mr LANGUILLER — Thank you.

Mr ELSBURY — This is an interesting one for you. What do you think the community’s expectation is around privacy?

Mr WATTS — In this context? I will try to characterise myself as a member of the public for a minute. I would like to have my cake and eat it too. I would actually like to see data, but there are competing public interests here. I would like to see data used to better inform research in relation to motor vehicle accidents and their outcomes — how to deal with them and ensure the carnage that goes on on our roads diminishes. The question is: how do you balance the two? How do you integrate the two?

I think it is often easy to look at these sorts of issues and characterise them as either/or choices, but there are winners and losers. I do not think that is the best way to look at them; I think the best way to look at them is, ‘We have two interests here; how do we satisfy both?’. There are techniques that you can use in data linkage projects to essentially make data anonymous.

One of the main difficulties with it is that technology moves so quickly. If you had to come up with a scheme in the year 2000, for example, it would be based on assumptions about computer techniques and technologies that are antique by now. The mobile phone in my pocket has more computing power than the one that was on my desk back in 2000. Technology is a movable feast and research into genetics and a whole range of medical issues also moves quickly. That is one of the difficulties in coming up with a formulaic solution to this particular problem. For a dynamic situation, you need to look at privacy protection in an environment where technology changes.

To go back to the thrust of your question, it is obviously an incredibly important public interest. How do you satisfy that and protect privacy at the same time? I do not believe there have to be winners and losers.

Mr ELSBURY — It is kind of like the Australia Card debate really, is it not? It was a be-all and end-all identification card, but ultimately people were not comfortable with the idea of it all being in one place.

Mr WATTS — Yes, that is right, but more recently there was the access card. If you remember there was a proposal for an access card back in 2006 or 2007 which, for a variety of reasons, did not come to fruition. What is very interesting is the commonwealth has actually learnt to do the things that I am saying should be done — that is, without extensive legislative amendment try to work with the legislation that you have to produce the sorts of outcomes that you need. The commonwealth has actually been quite sophisticated. I never thought that I would ever say this in the entirety of my life, but I think the commonwealth is ahead of us on this.

Mr ELSBURY — That is a scary thought.

Mr LANGUILLER — Through the Chair, can you briefly explain why?

Mr WATTS — I think these sorts of data-sharing issues have raised their heads lots of times within the commonwealth, to the embarrassment of bureaucrats and politicians. I think they have been able to take a much more nuanced approach to these sorts of issues and actually buckle down and do some of the things I am suggesting should be done — that is, to try to work within legislation but look at issues of legal authority and make sure they are broad enough and to make sure that organisations that are empowered and funded to do research actually have the tools at their disposal to do so and at the same time to protect privacy. As I said before, it is not an either/or situation. I think both public interests can be satisfied.

Mr ELSBURY — As you were saying earlier on, the general public would think that privacy legislation would be the be-all and end-all, but each department should look at the jurisdictional powers before they start making decisions on these things. A number of witnesses have indicated to the committee that there is an inconsistent interpretation and application of privacy law across government departments and agencies, and concerns have also been raised that while legitimate privacy concerns exist, often the perception of how privacy should be protected can act as a barrier to data being shared across agencies. What is your response to these concerns?

Mr WATTS — My first response goes back to the initial point I make. Each government department is unique because each has its own empowering legislation and its own legislation that gives it authority to collect and use and disclose information. Apart from its empowering legislation, there is a whole range of legislation that sits around it that governs or restricts the way information is used. So in a very real sense, when you talk about information sharing, each government department comes to the table with a whole set of different rules; it is not as if the landscape is exactly the same for each. There is insufficient discussion, I would have thought, and thrashing through of those issues within government and within departments. That is the first point I would make: there is insufficient meeting of minds and thinking through the information-sharing issues that need to be dealt with.

The second point I would make is that that is caused by flaws in governance, in my view. Various regulators — the Ombudsman, the Auditor-General and I, in respect of Victoria Police — have pointed out flaws in the way we go about governing our use of information within the public sector. Information is an asset, just as finances are an asset and just as human resources are an asset within government. We are slow catching up in looking at what governance you actually have to use over information to make sure that it is dealt with appropriately, to make sure that it is used as an asset to the people of Victoria and to achieve the sort of public interest balancing you are talking about.

That is related a bit to flaws in ICT governance, because ICT is the way these issues are dealt with if we use technology to do this complex information linkage or complex information sharing. There have been so many failures in Victoria but also elsewhere; we are not on alone on this. ICT projects and their governance and the information flows through them are often seen just as technology projects. Really they are information projects, and you have to look at them from the business perspective rather than a technical perspective. In putting together an information-sharing scheme, if that is a good way to characterise it, we have to go back and look at some of the fundamental issues. Some of the fundamental issues are ICT governance; information governance and the recognition of information as an asset to the state and an asset in dealing with significant public policy

issues, like road safety; and getting ourselves organised around those sorts of issues. Those are key issues. Does that answer your question?

Mr ELSBURY — I think so, yes. That is a very comprehensive answer to that particular question.

Mr PERERA — In the evidence received by the committee there is a strong theme around linking data from different government agencies to ensure better reporting and analyses of crash-related data. While a number of projects that link two or more datasets exist, there have been calls for a more structured process to facilitate ongoing data linkage. From a privacy perspective, are there any issues that may arise from establishing formal coordination between government agencies, including appropriate governance over privacy of information and the exchange of data?

Mr WATTS — Part of my answer to that question goes back to what I just said about governance. I make the observation that information governance within the public sector is suboptimal, but as a subset of that I also make the point that privacy governance within the public sector leaves a bit to be desired, and so does security governance. It is difficult to discern on occasions. Whilst there are theoretical reporting lines within government departments, it is actually difficult to find people at a senior level — not at a junior officer level but at a senior level — who sit at the executive table and who actually have a good working knowledge of what the issues are and the sorts of issues we are discussing today.

That is one of the issues in relation to governance. We do not see information as the asset that it is, and there needs to be a sea change in our attitudes to that. Information is fundamental to the way we improve policy, the way we improve the implementation of policy and to measuring outcomes. Those are key things. I do not believe privacy stands in the way of that. I think people need to work with it in a nuanced way.

To get back to the first part of your question, yes, there are a number of structured processes that can take place. I have only come to this position of acting privacy commissioner somewhat recently, but I can say this to you: for 10 years the Office of the Victorian Privacy Commissioner has been the only regulator in the country that has actually done training of staff within agencies for free. We do enormous amounts of that. In coming to look at that recently I started to ask myself the question: is that targeted at the right area? Should we be looking at actually teaching people and teaching officers at a more senior level how to work through the thorny problems?

As you are probably aware, the government announced late last year that it would develop a privacy and data retention office. That is under way. That is one of the things that is on my agenda for that new role — to target training at a high level within government, teaching people how to work with privacy and to do the sorts of things I have been saying to the committee. Do not start with privacy; look at your legal authority. Peter Carver has heard me say that many times. I think we need to do that, and I think that is an obligation I have going forward.

I think with these particularly complex areas that the committee is grappling with, one of the things we could do to assist is to actually bring the relevant parties together and say, 'Let's sit down and have a very frank conversation about what the issues are'. Everyone who is involved or wishes to be part of some data-sharing scheme needs to put their cards on the table and say, 'Here's what our legal authority is. Here's what our lawyers tell us about risk' — and different lawyers say different things about risk, and different secretaries interpret advice differently — 'This is what our IT people say about it. This is what our policy people say about it' and try to develop a common approach.

The only caveat I add to that is that as a regulator I have to walk a very fine line between advising people and then being in the embarrassing position of having to rule on my own advice, which I do not fancy, or pushing people in the right direction, asking the right questions and making sure they have covered off all the bases — and requiring them to go through, in these really complex situations, the due diligence processes that are necessary to manage the risks.

There are tools to do that. We as an office give advice, and there is information and guidance that we provide, but the way you do that with privacy is through a thing called a privacy impact assessment. The way you do it in a security sense is with an information security threat and risk assessment. You look at the risks, isolate the risks and then come up with mitigation strategies and work out what is and is not possible. That process might, in some of the circumstances the committee is considering, say, 'There's a problem with legislation. We need to do something about the authorising legislation. There may need to be some amendment to it to permit this type

of information sharing'. I would recommend that process because then everyone is across what the issues are. They all understand what their information flows are. They all know what the legal obligations are, they have got to the table and you can manage risk across all of them.

To the extent that that is possible, I am happy to broker that. I am happy to sit down with people at a workshop, a seminar or whatever is most appropriate and say, 'Here's the right way to go. Here's the right approach. Go away and do it'. That is what I can do, and I am very happy to facilitate that. I cannot speak on behalf of the health services commissioner, but he is a very reasonable person and I am sure he would be happy to facilitate that.

Mr PERERA — Who are the people your office trains? All the government agencies? You mentioned that your office is training people.

Mr WATTS — We train public sector agencies, local government, schools, universities et cetera. We are the only office in the country that does it, and we do it for free. Lots of people attend. We hold network meetings every six months or so, and everyone gets together and shares views, but what we do not cover at the moment are the more sophisticated, difficult issues this committee is grappling with.

Mr PERERA — In establishing such formal coordination, is it feasible to establish tiers of access where the privacy requirements around the release of data between government agencies might be less rigorous compared to the requirements for the release of data from government agencies to external agencies such as research schools?

Mr WATTS — The answer to that is no, and the reason is that it creates boundary issues. It creates additional complexity in an area that is really complex as it is. You can see from the briefing I have given you that there are a range of intersecting commonwealth and state laws. It just creates more complexity, and I do not actually think it is likely to improve on what I have been suggesting so far. If those who are party to an information-sharing initiative got together and worked out what the risks were and how to navigate through them, you would get the outcome you need, rather than having a two-tiered type of system. It superficially sounds attractive, but I do not think it actually provides you with what you need.

Mr PERERA — On what basis, if any, would the linking of two distinct datasets not be possible under the Information Privacy Act 2000 or the Health Records Act 2001?

Mr WATTS — The answer is that it is possible, but there are security issues associated with it. Within the one physical server — the one piece of equipment — you are trying to apply disparate security ratings. That is possible, but it may be complex and may not be needed. It is a potential answer to the problem, but it is not the answer. The question is, 'How do we go about sharing information?', not, 'Where do we store it?'. Do we store it in the top drawer, which is unlocked, or the bottom drawer, which is locked? I think it goes to storage, but I do not know that it necessarily goes to the up-front question you are concerned about.

Mr PERERA — What examples exist of formal coordination around data exchange between government agencies and departments for linking purposes in Victoria?

Mr WATTS — I am not sure about that. The Department of Health may have developed those sorts of arrangements in the years since I left it, which is now six or seven years, but I will address that question more generally. Questions of sharing data between Victorian government agencies have been quite problematic. My deepest recent experience was with security in Victoria Police. One of the things Victoria Police is permitted to do is share information — it has much more latitude than most agencies — but the security standards require that, if it is going to share information, the recipient of that information has to provide the same degree of security that Victoria Police does. That sounds really simple, but it has taken Victoria Police five years to develop an approach to it and to get those agreements signed off. It sounds simple, but sometimes it can be difficult.

When I say that one of the things I can do to assist is to bring people together, to get them all to put their cards on the table and to suggest a way to navigate through some of the issues, that is based on that experience with Victoria Police — the difficulties they have had in dealing with those issues. They are now getting there. Our degree of sophistication is growing but our maturity is not there yet, and that is why I say that the commonwealth is ahead of us.

The CHAIR — There has been some discussion in the evidence around the possibility of integrating datasets whereby data would be collected in a standardised and centralised way and stored in a data warehouse. It is claimed the adoption of this system would require decision-makers to overcome the perceptions of problems with privacy, access and control. You may have already addressed some of these issues in earlier commentary, but my question is: what issues regarding privacy may arise from integrating datasets?

Mr WATTS — Ultimately it is a question of legal authority. If Victoria set up a data linkage authority for motor vehicle accidents, for example, and said the authority was empowered to collect X, Y and Z information and to provide advice to government and to researchers et cetera, then that would absolutely become possible. However, it has been presented to you as a technological solution — let us put many different datasets in a database. I can hear the chief information officers of many government departments saying, ‘That’s fantastic. Let’s put it all in one database and interrogate it’. But who owns it? Who is responsible for it? Who looks after that database? Ultimately it is a technical solution looking for a policy solution, and what needs to sit over the top of that is the policy solution.

Before I go — and I am conscious I am taking up your time — there are some other things, and I will mention them just briefly, that can be done in the last resort if there is not sufficient flexibility or if privacy is found to stand in the way of pursuing a proper public interest. One is to introduce some flexibility into the privacy act. It is meant to have some flexibility built into it. It provides the ability to develop codes that apply to particular schemes of information sharing within a particular subject matter area. Those provisions have never been used and one of the reasons is that you can only increase privacy protection, rather than ratchet some down and ratchet others up to produce overall a compliant privacy outcome. Some flexibility around code provisions is one way of doing that.

Another way that is found in other privacy legislation and is also found in trade practices legislation is through authorisation provisions. You may be aware that the ACCC, as the old Trade Practices Commission, used to be able to authorise certain breaches of the Trade Practices Act in the public interest, if there was a demonstrated public interest. There is an approach that has been taken by New Zealand most recently, particularly to address information-sharing issues around child protection — that is to develop schemes of approved information-sharing agreements, which allow you, for public interest purposes, to devise a scheme again that protects privacy but might depart from privacy or the strict letter of privacy in certain circumstances. They can be developed. Obviously people need to make submissions about the public interest in doing that. They go to the privacy commissioner for assessment and then ultimately to the minister for sign off.

If you want me to leave you with any message today about privacy law, it is that mostly it does not stand in the way. People find it difficult to deal with. It is not all privacy’s fault; it is the fault of other legislation is well and that needs to be navigated. On the occasions when it does stand in the way of legitimate and important public interest, then some flexibility is in order, and you can do it.

The CHAIR — Mr Watts, thank you very much for your contribution today, your additional suggestions, your overview of the subject matter coming from a very strong sector background as well as the information paper you have circulated today, will be of great help to our staff. On behalf of my colleagues, thank you for your time.

Mr WATTS — If there is anything further, please do not hesitate to let me know.

The CHAIR — Thank you.

Witness withdrew.