T R A N S C R I P T

LEGISLATIVE COUNCIL LEGAL AND SOCIAL ISSUES COMMITTEE

Inquiry into Management of Child Sex Offender Information

Melbourne—Thursday, 22 April 2021

MEMBERS

Ms Fiona Patten—Chair
Dr Tien Kieu—Deputy Chair
Ms Jane Garrett
Ms Wendy Lovell
Ms Tania Maxwell
Mr Craig Ondarchie
Ms Kaushaliya Vaghela

PARTICIPATING MEMBERS

Dr Matthew Bach
Ms Melina Bath
Mr Rodney Barton
Ms Georgie Crozier
Dr Catherine Cumming
Mr Enver Erdogan
Mr Stuart Grimley
Mr David Limbrick
Mr Edward O'Donohue
Mr Tim Quilty
Dr Samantha Ratnam
Ms Harriet Shing
Mr Lee Tarlamis
Ms Sheena Watt

WITNESSES

Mr Sven Bluemmel, Victorian Information Commissioner, and

Ms Rachel Dixon, Privacy and Data Protection Deputy Commissioner, Office of the Victorian Information Commissioner.

The CHAIR: Good afternoon, everyone, and welcome back to the Legislative Council Legal and Social Issues Committee's public hearing for the Inquiry into Management of Child Sex Offender Information. Again, mobile phones, please ensure that they are turned off.

Welcome back to any members of the public who are watching us online today. I would like to welcome our next witnesses from the Office of the Victorian Information Commissioner. We have got Commissioner Sven Bluemmel and Deputy Commissioner Rachel Dixon. Thank you very much for joining us today.

I am joined here today by my committee colleagues Kaushaliya Vaghela and Sheena Watt. We have Deputy Chair Dr Tien Kieu online, and Mr Ed O'Donohue and Mr Stuart Grimley here with us today.

If I could just let you know that all evidence taken is protected by parliamentary privilege as provided by our *Constitution Act* but also by the standing orders of the Legislative Council. This means that any information you provide here today is protected by law. However, if you were to repeat the same things outside this place, you may not have the same protection. Any deliberately false evidence or misleading of the committee may be considered a contempt of Parliament.

As you can see, we are recording and broadcasting. We will provide a transcript of this hearing to you in a little while, and I would encourage you to have a read of it, just to ensure that we have not misheard or misrepresented anything that you might say today.

We would welcome some opening remarks, and then we will open it up to a committee discussion. Thank you very much.

Mr BLUEMMEL: Thank you, Chair. It is a pleasure to be here. Thank you to the committee for the opportunity. We are very pleased to provide evidence here today, and we hope we can be of some assistance in your deliberations.

Just by way of background, we are of course the independent regulator in Victoria of freedom of information, information privacy and information security under the FOI and the *Privacy and Data Protection Act*. Anything to do with the proper use of and protection of information is of course clearly of great interest to us, so we are pleased to be here.

We have made a written submission to the committee. I obviously will not go through the full content of that. I would just like to highlight a couple of points. In our submission we specifically considered how offender information is currently maintained on the register. We outlined some considerations for storing and managing the information and then, perhaps of greatest interest, the considerations for potential broader access to the information beyond what is currently there. So that relates squarely to terms of reference a) and c).

Now of course this is a very sensitive and complex area. I suspect that probably every witness has said that, and of course it is right. We are certainly not proposing to go through the arguments for or against broader disclosure. Where we think we can add some value to your deliberations is to talk about the key considerations from an information security, information handling and privacy perspective that will be useful for you. Of course we also referred extensively to the Victorian Auditor-General's Office report of I think 2019, which highlighted some of the issues around how the register is currently kept, the sources and how they are linked.

For us, just briefly starting with that, and I will keep my remarks brief, the issue of data quality is a very important one, particularly so in this very sensitive context where incorrect data can have some very harmful effects both to the systems but also of course to individuals. When a system is distributed, as by necessity it currently is, then that does from our perspective increase the information security risks, the data quality risks. It increases the vectors for potential attack and so on. So clearly that is an issue that was highlighted by the Auditor-General, and we certainly agree.

Now, Victoria Police of course is subject to the *Victorian Protective Data Security Framework*, which is under our *Privacy and Data Protection Act*, and we have oversight of that so that falls squarely within our jurisdiction. In Victoria the *Privacy and Data Protection Act* is the primary privacy piece of legislation under which both Rachel Dixon and I have roles to play as statutory officers. General principles of that include that the use of information be necessary and proportionate to the outcome that is to be achieved here—of course the protection of children from harm. The considerations for us are minimising and ideally avoiding unintended negative consequences. As has been highlighted in our submission, the sorts of unintended consequences that may occur with public or greater public access to a register like this are potentially negative impacts on existing victims who may be identifiable, potentially retraumatising of those victims from identifying their assailant, potential vigilantism and so on, but also a potential false sense of security—what inference is drawn from the fact that somebody is not on a publicly available register, and is that inference justified?

Those are our considerations broadly speaking. There are then some decisions that clearly need to be made if there is to be some public access about how that is to be done, and the sorts of considerations are of course how much information should be disclosed, what kind of offenders are to be subject to a scheme like that, who can access that information, how is that access provided and are there any restrictions on how the access to information can be used.

That is all I wanted to say by way of introductory comment, but of course we are very happy to take any questions you have.

The CHAIR: Thank you very much and yes, thank you for your submission. We have all got copies of that. In the current circumstances the police may release information and disclose people on the register if they think it is in the public interest. In your view, do you think how it has been used to date has been effective and has not breached any privacy conditions as it is used today?

Mr BLUEMMEL: I think broadly in terms of the effectiveness, it is probably not for us to really express a view on that in terms of the effectiveness of reducing harm. We are simply not the experts in that regard. In terms of the data handling and privacy aspect of that, currently speaking given the fact that access is restricted by specific legislation broadly means for us that the privacy risks in that regard are being managed, if I can put it that way. Rachel, I do not know if you like to add to that.

Ms DIXON: No, I think it is exactly right, and I think you alluded to this earlier. The big issue is if you are wanting more and more information made available to the public in any kind of sense than currently exists, you have got to deal with the fact that there will be a lot of cases where, for example, Victoria Police currently will not publish that information because it may reveal the name of a victim. Now, that means that by definition anything that was published to the public will only be a small slice of the actual offenders that you have got, and I think one of the submissions that your committee received referred to the Western Australia scheme and gave a figure of 6 per cent. That will probably give the public a false sense of security. In the way the current scheme works I think it is managed professionally. Victoria Police have to make that risk assessment in terms of the potential harm to victims, and so far it seems to be running reasonably well. But stepping outside of that I think would raise some fairly significant concerns for us in terms of the victims' rights.

The CHAIR: Thank you. I will move to my Deputy Chair, Tien Kieu.

Dr KIEU: Thank you, Chair. Thank you both for submitting the evidence and appearing here today. Given that you have submitted about the collection, the storage, the accessibility of the information, the integrity and also the security, I would like to have your opinions on whether you have any concerns about the aspect of cybersecurity for the system. Also in connection to that—I have asked the question before with the police—the registry is to monitor and track the offenders when they are released back into the community for the protection of the public and also for the safety of the public, but now people can access the internet, the sexual gratification of some of the criminal activities can be done not in a physical way but more over the internet. So do you think that the present arrangement for internet accessibility for those on the register is satisfied or not? Is there anything that we should do more?

Mr BLUEMMEL: Well, I think generally the issues were highlighted by the Auditor, about the distributed nature of the system currently, including the fact that there are quite a large number of records in hard copy in fact. Now, that was a couple of years ago; I am not sure of the current status of that. But the more distributed it is like that, the more there are points where things can go wrong. Now, there are also downsides to centralising

everything. The more you centralise it, the greater the honey-pot effect is and the bigger and more valuable the target is for an adverse actor. So in terms of whether it is currently being managed securely, I think we would never be in the position where we could say, 'Yes, it's secure. It's all done. There's no need to worry about it'. Given the sorts of things that we administer and the sorts of events that we see, there is always a level of risk. So broadly speaking, I think at the moment because the exposure of the data to the internet more broadly is limited—very limited—that risk is smaller. If something were to be exposed more broadly for public perusal or search or even logging in, that risk increases. That is what I would say by way of an overall assumption.

Ms DIXON: To be clear, the protective data security framework that Victoria Police abide by—the same as every other government agency now—is a risk-based framework. So as part of preparing that framework every agency—VicPol is no exception—has to essentially develop a list of all of the information assets they hold and assign risk ratings to what would happen if this information was exposed. Now, Victoria Police obviously have a lot of very sensitive systems and they would be a very attractive target for a cybercriminal, so there is no way you can say that something cannot be hacked. It is certainly possible. However, Victoria Police's plan has to assign a high degree of risk to that material being made public. We would think that would be consistent with appropriate behaviour. As Sven has said, the problem at the moment would seem to be that there is a lot of manual copying, so there is a data integrity issue, I think, that so far appears to be being managed, but we cannot promise that that will always be the case. It is very easy to transpose a keystroke or misread something when you are copying it from one thing to another. That is obviously not optimal. As Sven has said, the only plus side to that is that if it were to be hacked they would only get part of the information. So, you know, it is swings and roundabouts, but it is risk based; there is no absolute.

Dr KIEU: In your submission you mentioned the 2019 VAGO report and recommendations. Have you had any involvement or interaction with the police about their data collection, storage and accessibility?

Ms DIXON: My team has a regular monthly meeting with VicPol, and certainly information handling generally has been a topic for discussion. We have not specifically homed in on the sex offender registry information, but we have had lots of discussions. VicPol recently, for example, cleaned out one of its document stores, moved to another facility, and we had several briefings from them about the progress of that. They also changed data centres a while back as well, and so we were obviously briefed on the transition from one data centre to another and the risk management process that was part of that. So not specifically on the sex offender registry, but there are many other, as I say, VicPol systems that are also sensitive that we expect the same standards would apply to.

Dr KIEU: I hope that the data centre is based in Victoria or at least Australia and not overseas.

Ms DIXON: It is not overseas. I will not say exactly where it is, but it is not overseas.

Dr KIEU: Okay. Let me come back to the second part of my question just now. The availability and accessibility for people who are on the register—internet accessibility—is it a concern for you?

Mr BLUEMMEL: Would it be a concern for us if it is made available?

Dr KIEU: No, no—whether they have direct and easy access to the internet so that some of them may groom or do some video or texting or whatever to satisfy their sexual gratification. Because the registry is to monitor and track people, but that is physical location and their physical movement, but now people do not need to do that—they can have access from anywhere and to any corner of the world—so should that be something of concern to you and how should we deal with that?

Mr BLUEMMEL: Certainly the ability of an offender or a potential offender to get access to this sort of material or indeed to communicate one on one with a potential victim through digital channels would certainly be a concern. It starts going for us, though, outside of our jurisdiction really because we are about the handling of information by the Victorian public sector—in this case the police and other related agencies. So in the most general sense, yes, I can certainly see that that is a very real concern and very real harms can come from online interactions—absolutely. Of course even the creation of a demand for that sort of material will produce victims along the way who are then subject, unfortunately, to that material. So I can certainly see that as a very real concern, but I think in most cases that would be something that would be outside our remit to regulate.

Dr KIEU: Yes. Chair may I have a quick question next, or should I wait?

The CHAIR: We will probably come back to you, Tien, if that is suitable.

Dr KIEU: Thank you, Chair.

The CHAIR: Thank you. Mr O'Donohue.

Mr O'DONOHUE: Thank you, Chair. Thank you both for being here today. I am interested in your role in the data compliance and ensuring data security, and I note the comments that the data protection framework is risk based so it is impossible I suppose to give any sort of guarantee about the risks. I suppose that is a dynamic thing. It can change quickly too, depending on someone's mistakes or errors et cetera. VicPol has invested in some significant changes in its data management. There is a new integrated intelligence system procured from SAS, there is the Interpose system and LEAP continues to operate. We have talked about the honey-pot effect and the benefit of having multiple sources of data in that it reduces the risk if there is an exposure, but what is the risk of having multiple systems operating? Does that create a weakness in the system if there are multiple data systems working across different platforms?

Ms DIXON: One of the problems—sorry, Sven—that any organisation faces when they are going from an older system to a newer system is the point at which the old system becomes less useful. Can you ever turn it off? Banks, for example, face this all the time. They are using computers made in the 1970s to still process a lot of information. The Neo platform that VicPol currently uses actually receives information from Interpose and LEAP as well, so there is now at VicPol this sort of single source of truth—not all of the data, as we have seen in some of the submissions. For example, VAGO found that some of this data was still being held on paper because that historical stuff will take a long time to get into Neo or any of the other systems. It will go into Neo, my understanding is, as information is digitised, and of course as new cases come in they start in Neo, not necessarily in LEAP and Interpose anymore.

We had a briefing on how that architecture works. I will say that one thing that we did put into the standard the year before last, when the Special Minister of State signed the new standard version 2.0 of our framework, is that we actually put in place a notification standard such that if there are any breaches of any system that have a business impact level of two or higher—and there is a way you can calculate that, which means essentially anything that has the potential to have some sort of serious harm—it must be reported to our office. Now, if it is a cyber incident, we do a 'no wrong door'. They can report it to DPC's cyber unit for investigation, because they have a 24-hour service. Obviously with a cyber incident you want to get onto it really quickly. But if it is just something like a lost file or if it is a radio being lost, they all get reported to us. We have a weekly stand-up where we assess those things, and then we will ask follow-up questions of VicPol.

So this system, all of these systems that they are currently using—if there is a breach in relation to any of those things, VicPol are obliged to notify us of any serious incidents, and then we will ask relevant questions. We can at the moment also look up some of the incidents ourselves. We actually have access to VicPol terminals so we can see what those incidents might relate to, which saves us having to go back 300 times to ask them lots of questions about fairly simple things. Victoria Police run a fairly substantial operation and there are lots of incidents, just by the nature of that many police officers.

Mr BLUEMMEL: With the other thing, just by way of risk context, the framework is indeed risk based, and that was a very deliberate decision. But often the risks are around the periphery. It is not cracking the encrypted data on the system with a brute-force attack. I mean, yes, that does happen, but it is actually relatively rare. It is all of the touchpoints where people sit at a machine and enter information or where the systems are such that individual officers may start developing parallel systems where they write things out by hand so that they have it to hand, and then of course that becomes a risky document that may be breached. So all of these things are factors. It is rarely at the heart; it is often at the interface between systems and humans or indeed, in this case, between systems as there is transition.

Mr O'DONOHUE: If I may, Chair, just on that, I have had information from within the department of justice that Cenitex continues to be an ongoing challenge, an ongoing issue, in its provision of service. The department of justice would interact through corrections and other limbs of justice into VicPol systems about these offenders in this case we are discussing today. To further your point, Sven, how much of a risk is that, given that perhaps other parts of government do not have the same systems, I assume, from what I am reported?

Ms DIXON: Cenitex provides services to a great many government agencies, I have to say.

Mr O'DONOHUE: They do.

Ms DIXON: Yes, Cenitex is quite a big operation.

Mr O'DONOHUE: Yes, very big.

Ms DIXON: Look, again, I have to say we do work with agencies where there have been incidents to try and get them to work out what the risk profile is on some of those things. Without going into specific details about specific incidents, there have been other areas of justice that have had some degree of compromise from time to time. We work, then, with them to make sure that that risk is mitigated and will not occur again. These are not regular. As Sven said, it is usually human error in one way, shape or form.

Mr O'DONOHUE: Do you report publicly the levels of breaches?

Ms DIXON: We report the number of incidents and we report the severity of incidents. For obvious reasons we do not tend to report the detail of those incidents. What we do have, one of the weaknesses I think in Victorian legislation, is that in our privacy Act there is no positive obligation to notify people whose information may have been breached. We encourage agencies to notify individuals, but there is no positive obligation in our Act. There is in many other jurisdictions.

Mr O'DONOHUE: I have got one final question. Obviously the role you play, the statutory functions you fulfil and your interaction with agencies, including VicPol, are critical to protecting data, and the data we are talking about is so sensitive, as so much is. Do you have the resources to do it, because with the greatest respect I have noticed through the FOI process you are obviously stretched?

Mr BLUEMMEL: We certainly are stretched. We obviously try and optimise the different functions that we have both across the jurisdictions that we administer but then even within those jurisdictions, where there is some proactive work, there is reactive work and things in between, so obviously we try and manage that as best we can. One of the things that we are trying to do with our limited resources is, yes, we have to respond to complaints and so on statutorily, but we are trying to put in a lot more effort to get agencies to do things right in the first place. As Rachel has mentioned, what we learn from those data breach reports that we receive—and we learn a lot from them about what the nature of the risk is and how it is constantly changing—we then try and go to as many agencies that could benefit from it as possible to say, 'Here's what you can do to reduce the risk. Here's what you can do', and that is really important to us. Do we have enough resources? Look, of course with more resources we could do more and we could do it more quickly. I think that is always the case.

Mr O'DONOHUE: Would you like to put a figure on that? It is April.

Mr BLUEMMEL: Look, we have not done the 'here would be the ideal model and here is how much it would cost', because we think we have to do the best with what we have. Where there is a strong case to ask for more of course we do so.

Mr O'DONOHUE: Well said.

The CHAIR: Thank you. Kaushaliya Vaghela.

Ms VAGHELA: Thanks, Chair. Thanks, Sven and Rachel, for your submission, and it is good to see you in person. Western Australia has public disclosure enabling limited public access to sex offender information. In your view is there particular sex offender information which should be kept confidential within any type of scheme, and if yes or no, why?

Mr BLUEMMEL: Look, it is hard to say. We have not gone to that level of granularity specifically, but what I would suggest in line with my opening comments particularly is we need to answer that question by reference to the harms we are trying to avoid. So, for example, one thing we clearly all want to avoid is further harm to an existing victim. Information that might, if made available, have some adverse effect on the victim either by way of details about the events or sensitive information about them at the time—their age, those sorts of things. I would say there would be a very strong case for that not to be available because that could have a really bad impact on the victim. That is one thing that immediately comes to mind. I think Western Australia, which has now been operating a scheme for a few years, would certainly be worth exploring. If I am correct, I

think they have undertaken an initial review of that scheme, so that might be a good place to look. I probably have not got anything further in turns of specific detail.

Ms DIXON: Just to back Sven up, I think one of the things is if information is made public, then obviously the photographs of the offenders can be provided as well. I think one of the last things you would want as a victim is to be walking down the street and see the photo of your offender staring back at you. I think there is certainly a risk there of continued trauma for the survivors, and I think that is something that we generally think is the most important thing to manage in this scheme.

Ms VAGHELA: So what are the elements of a successful public disclosure scheme? Would you have any things that should be part of a successful scheme?

Ms DIXON: I think that we come back to the thing that Sven raised before, which is: what is the purpose of the public notification? What are we trying to achieve with a public register? I think once you have established what that is then you can start to answer whether or not any scheme is providing that. We are not the criminologists; we do not have a background. I have noticed people have talked about the risk of recidivism not being reduced by public registers. So the question is: what is it for? What is a public register for? Who is it providing comfort to, and how can it be effective? And I think that is outside our sphere of expertise. That is why you are here.

Ms VAGHELA: Yes. We had one of the presenters here saying that AUSTRAC should have access to the register so that they are able to do some of the monitoring or detective work better. What are your thoughts on that?

Mr BLUEMMEL: Did you say AUSTRAC?

Ms VAGHELA: Yes.

Mr BLUEMMEL: Right. Well, I think for us from a privacy and data protection point of view—and we have not thought about this specific example—that would be at the controlled end of the spectrum and therefore the risks. So where you have a government or a cross-jurisdictional agency that has a particular need to access information for a particular public purpose, then that is much more manageable than something that is public or semi-public. So I think if there were a case there—and I am obviously not familiar with the arguments there—then that is at the lower end of privacy risk than anything that is browsable or downloadable.

Ms VAGHELA: Yes. The example they were giving is, say, if someone has bought software online and then that particular perpetrator goes and buys a plane ticket. If someone is monitoring the activity, if AUSTRAC has access to that, then they are able to follow and track what that person is doing. So that was the example they had given in their submission.

Mr BLUEMMEL: And I guess that is a bit like things like terrorism financing and those sorts of things—the money flows together with other pieces of intelligence. I can see how an argument like that could be constructed. And again for us, dealing there with a government agency with a specific legislative remit is then a risk that can generally be managed through legislation, through an oversight body and so on, to make sure that that is not being abused.

Ms VAGHELA: I have got more questions, but in the second round.

The CHAIR: Stuart Grimley?

Mr GRIMLEY: Thank you, Chair. Thank you for your submission today. It is nice to see you both. You spoke before about the photographs of offenders and their potential impact on victims, especially if they see those photographs out in public—the impact that that may have on victims. Victoria Police have released publicly a number of photographs in recent times of registered sex offenders that have gone missing, in the interests of public safety. Has OVIC become aware of any instances of issues pertaining to the release of that information at all?

Mr BLUEMMEL: I do not think we have specifically, and I think we probably would not. For example, if that were released and then there was some traumatising or retraumatising of existing victims, I would not expect that to find its way back to us by way of a complaint or a process like that. So it may or may not happen,

but we may not necessarily be aware of it. And I note in that regard that the Western Australian one, for example, has some safeguards against that, because you can get access to photos in certain cases, but I believe the photos are then also watermarked with the person to whom they are released to provide a track-back, and there are restrictions against using them for public on-posting and so on.

But I think in the example you have given there, again we always look at what is necessary and proportionate, and in that example there, where offenders have gone missing, I think there is then a stronger case to be made to say, 'Well, public release here, that has tipped the balance in favour of public release because this person is missing, we know they are a risk and we need the public to help us track them down'. That is sort of a particular use case where that is stronger than for a general person who is on the register—so again that proportionality.

Mr GRIMLEY: Yes, that is right. So the proportionality between the risk to the community as opposed to—I do not know if that is the right word or not—the impact or the potential impact on a victim has to be taken into consideration, and in instances where the community is at risk then that information can be released publicly. Thanks for that.

I also note in your submission you referenced the VAGO report which found that data in the sex offender register is held across multiple systems, like Mr O'Donohue was saying before. They report that it is not well integrated and is entered in a manner which increases the risk of inaccuracies or incomplete records, like you said before, and the duplication of data et cetera. You spoke briefly about the register and how you believe it is working satisfactorily—I am not too sure; they were not your exact words—or is working okay. Victoria Police report that registered sex offenders on the register are growing by around 500 per annum. Given that, do you think that data integrity or quality concerns will eventuate given the rise in those numbers per annum?

Mr BLUEMMEL: Well, certainly any rise would increase all of the risks, both the risks that we talk about with information integrity, data security and so on and also of course the risks of future offences potentially happening because there are offenders out there, so it certainly increases in that regard. In terms of just sort of clarifying whether we think it is working appropriately I think our comments were really confined to the fact that we have not received specific concerns or complaints or had to otherwise investigate whether the privacy and security issues about the current register are problematic. We have not had to do that, so in that sense whether it is achieving the criminology outcome is not something that we have looked at.

Mr GRIMLEY: And just one more if I can: we have also spoken about the breaches of access to police information; it has been brought up before in questions with other submitters. There are concerns that other organisations may be able to access information illegally. You did mention that it is publicly released—the number of breaches—but to your knowledge have any of these occurred specifically in relation to the sex offender registry?

Ms DIXON: I have been, I think, involved at OVIC for a little over three years; in my time we have received no notification of incidents regarding the sex offender registry.

Mr GRIMLEY: Thank you. Thanks, Chair.

The CHAIR: Sheena Watt.

Ms WATT: Thank you, Chair. I understand that Deputy Chair Tien Kieu has some additional questions, and I am happy to pass it over to the Deputy Chair of the committee.

The CHAIR: Okay. Thanks, Sheena—back to me. Just considering the West Australian model that you did mention in your submission, you mentioned that the people that that disclosure would apply to is a very small cohort of that group. If a similar system were to be proposed or enacted in Victoria, would that have any impact on our existing freedom of information legislation? Do you think we would require changes to other pieces of legislation to accommodate such disclosure?

Mr BLUEMMEL: Look, I think not necessarily. I mean, at the moment the content of the existing register is exempt from the Act. I would imagine that would remain regardless of any decisions to publish it. Are there other pieces of legislation that may be impacted? Possibly, but I think with FOI the way it already exists the exemptions that are in place are fairly broad in their expression. What we are trying to do is—

The CHAIR: Public safety or—

Mr BLUEMMEL: Exactly. And so what we are trying to do on the FOI side as the Office of the Victorian Information Commissioner is encourage agencies to interpret those exemptions much more narrowly than is sometimes the case, and we are going to continue doing that as much as we can. But with something like this I do not see a pressing need for any concomitant changes.

The CHAIR: No. And presumably one would be able to sufficiently argue that even under the protections that our charter provides, public safety would trump that.

Mr BLUEMMEL: Would trump that in terms of privacy or—

The CHAIR: Yes. If not disclosing that information put the public at risk, then disclosing that information would not be in breach of the charter.

Mr BLUEMMEL: I think that would be right if that conclusion were reached. Certainly the charter—and of course that is primarily administered by the equal opportunity and human rights commissioner. One of those rights of course is privacy, and we have the *Privacy and Data Protection Act*, but certainly that right is not absolute. In a law enforcement context quite frequently there are cases where if information we collected was used or disclosed in another context it may be a breach of privacy. Where that is properly done for a properly valid law enforcement purpose there are mechanisms in the *Privacy and Data Protection Act* to allow for that.

The CHAIR: Yes, of course. I have some similar concerns about—if we were to look at a very limited disclosure model—the possible false sense of security that that may instil if we say we can only really provide information about a very small percentage of people. Are there any other analogies or are there any other examples of similar circumstances where you would find that the scope of the disclosure is so limited as to either provide that false sense of security or to find that it does not really work?

Mr BLUEMMEL: I can probably give one on a fairly large global basis, which is privacy in general—the collection, use and disclosure of privacy, particularly in a technology context and in a social media context. Yes, occasionally and fortunately more frequently our attention is publicly drawn to a company having done the wrong thing and having misled its consumers about what would happen to their data, but I think anyone who thinks that they are the only times that privacy is indeed breached or consumers are indeed misled is sadly mistaken. On a larger scale, that might be an analogy.

The CHAIR: Thank you. Yes, I think that is. Our deputy, Tien Kieu.

Dr KIEU: Thank you, Chair. I would just like to make some remarks about the security, particularly the cybersecurity, of the system with the technology and also the need for duplication and redundancy of data centres for data recovery processes, for example. They are as strong only as the weakest link, and more often than not there is a human factor in that that is very difficult to predict and to prevent. Let me come back to privacy. You mentioned, Sven, that the people who are inadvertently impacted by a release of a piece of information need not be informed because the Act does not require that, so should we amend the Act to inform those people who have been impacted in some way because of some of the data breaches and security breaches?

Mr BLUEMMEL: Look, I think there would be an argument to do so, and I think it would improve the system somewhat, but there are a couple of qualifications to that. One, as Rachel has already mentioned, is in terms of data breaches. Under our *Victorian Protective Data Security Framework* and the standards that sit under that framework, there is now a standard requiring agencies to notify us at least, and we can then work with the agencies to suggest, in many cases, that they notify the person whose personal information was breached—if indeed that happened. The other thing also though is that if there were a legislative obligation on an agency that has breached someone's personal information to notify that individual, I can foresee circumstances where you would not want to notify the person. It may be that the risk is so low and the trauma of notification might actually be quite high in certain circumstances, and there is, again, that proportionality that we always talk about. I think a general obligation and a positive obligation, as Rachel has said, would be an improvement to our privacy laws, but it would need to be done and drafted with care to make sure that it is not absolute and allows for notification, where appropriate or as the default, but has certain cases where notification could cause more harm than good as well.

Dr KIEU: Yes. Also I would like to hear from you about the right to privacy of victims if the registry is made available publicly. How can we protect that, and have you any concerns about the rights of the victims? Not the offenders because obviously they would be made public for some reason, but the victims can be identified through that—maybe because the offender is related to them or maybe because some of the incidents are reported elsewhere, in the media.

Mr BLUEMMEL: Look, the short answer is, yes, we would be concerned about that, and we would want to respectfully suggest that any decision to make information like this public be cognisant of that risk. So, exactly as you have said, clearly any information that expressly identifies a victim, I think there is a strong case that that should never be made publicly available. But, as you say, there may be other contextual factors—that the information does not name the person but through information that might be publicly known, a person, a group of people or even the public more generally can then deduce the identity of the victim, and that is certainly something that I think should be guarded against.

Dr KIEU: Thank you, Chair.

The CHAIR: Thank you, Tien. Kaushaliya.

Ms VAGHELA: Sven, in your submission there is mention of the recording of data, storage, so different parts of the life cycle of the data—handling, management—and then you also talk about the data quality, accuracy and it has to be current as well. Nowhere do I see mention of the deletion or the destruction of the data. Is there a reason for this particular register? If, say, for example, a registrant passed away 20 years ago, there might be some need of a historical linkage to that particular person, but is there a reason why there is no time limit? Because right now it gets stored for an indefinite period.

Mr BLUEMMEL: I am not aware of the reasoning specifically behind that. What I would suggest is that the risk, again, is different where we are talking about a register that is accessible by certain agencies or offices for their functions, because that can be controlled and there may be an argument to say, 'Well, that does need to be kept indefinitely because there is limited access and there might be something investigated a few years down the track that might be unsolved', and things like that. The risk changes very much when that is potentially available to the public, either on request or through publication. And if it is available to the public, then I think we would argue that it has got to be necessary and proportionate. Is the ability to look up a deceased sex offender's history necessary and proportionate to minimising future harm? An argument would need to be made to justify that.

What we always suggest is that the more data you hold and the longer you hold it, the bigger the risk. There might be really good reasons for holding a lot of data for a long time, but it comes at a cost. And I am not talking about the monetary cost of storage; I am talking about the cost of the risk. If you do not have it, it cannot be breached while in your custody. So if there is a good reason to have it, well, that might be an acceptable cost; but if there is no benefit, or even no strong benefit, you would have to argue against that. From a privacy prospective also you could argue that having that information accessible from someone who is deceased—for example, if they have an unusual surname—might colour their children's prospects if someone finds that name on a register and misrepresents that or does not realise that it refers to a parent or a great-grandparent rather than the individual that you are concerned about. Those are all factors that I think should be considered.

Ms VAGHELA: I think with other jurisdictions we found that it was based on risk, so it is a time duration depending on what the offence was, how severe it was. Do you think that should also be taken into consideration over here?

Mr BLUEMMEL: Potentially. It should be looked at, and again, we are not the criminologists, so we do not know whether there is a pattern that lower level offending leads to high-level offending and things like that. Well, we do not know; it is not our area. But they are the sorts of factors that I think would be looked at.

Ms VAGHELA: And just a quick one: in terms of classifying different information, as Rachel mentioned, the information on the register of offenders is very sensitive, even for the victims as well. I do not know if the criminal record or the sex offence does need to be classified, because we classify so many different types of information as sensitive information. Does this information need to be classified under any of the categories, because you mentioned, Rachel, when there is a breach—I think you mentioned a level 2 breach—say, for example, there was a breach of the data from the sex register. If you published the information, how many

breaches there were or whatever frequency you did that, that would bring up under what category it was. So 'the breach related to this sort of information'. Is there a need to classify that?

Ms DIXON: I am sure I have read in one of the submissions to this committee the desire in some cases to not list offences by children, for example, like sexting and things like that, because they fall to a different threshold when they are under 18 from what they might for an adult. This is a matter again for criminologists, I suggest, and the psychologists to tell you whether there is a risk in that or not. It is not for us to say that. As to whether or not some of the information on offences is more sensitive than others, it comes back to the issue that we have raised before, which is: what is the potential impact to the victim? That would be the thing I would be paying most attention to rather than the offender.

Just to follow on briefly, where there is a legislative exception, information can be retained for a long time. But I should just say one of the information privacy principles is that agencies should destroy data that is no longer needed for a particular purpose.

Ms VAGHELA: Yes, and that was my question.

Ms DIXON: Now, PROV, the Public Record Office, obviously has its own requirements, so there is a separate piece going with that. But once the offender is dead, the chance that they will be recidivist is probably fairly slim. There may be other reasons to retain that data, and the organisation would need to, maybe for example, for criminal research, for various—those arguments can be made, but then that information should only be used for that purpose. It does not mean that it should then be made available everywhere. The reason the IPP, the information privacy principles, exist is that they are principles based, and unless there is a legislative exception we would expect agencies to abide by those.

Mr BLUEMMEL: And I should also just note for broader context we do have an information classification scheme in Victoria, but from, for example, a transparency point of view what that does is show a judgement has been made about the consequences of a breach—if this document were inappropriately released or disclosed—but that inherently, under the FOI jurisdiction, which did come up earlier, does not make a document exempt under FOI. So regardless of what markings a document has on it or what level of classification it has been classified to, whether it is exempt under FOI or not will turn on the exemptions in the FOI not the document marking. It is just an important thing to note.

The CHAIR: Thank you. Stuart Grimley.

Mr GRIMLEY: Thanks, Chair. Just going on about the impacts of victims that you mentioned, as we know there are many high-profile victims that have come out in recent times who are more than happy to name their offender and perpetrator in the interests of protecting others from being assaulted. So, given that, how should those victims or survivors of sexual assault and their rights, I suppose, be addressed in this manner, in terms of the releasing of public information?

Mr BLUEMMEL:Well, I think in a case like that, where an individual victim-survivor has made his or her own choice to say, 'I'm going public with this', that is their choice. If that person is or is not on the register is not directly relevant to their choice as to whether to name them. I mean, there are others issues—defamation and so on—of course in certain cases. But in terms of the register I think the difference there is that one victim-survivor may want to do that and may want to go public and do that for prevention of future harm to others; another victim-survivor in a similar situation may not want to do that and to have a register do it for them. It is just a different dynamic. I do not see that anything here would change whether a person can choose himself or herself to name their perpetrator; I do not think it would change that. That is my understanding of it.

Mr GRIMLEY: Okay. And so just sort of moving from that, and you may or may not be able to answer this question, in terms of unofficial information that is available currently on the internet—there is plenty of it—in terms of so-called 'sex offenders in my community', how does that fall under the umbrella, if it does, of OVIC in terms of managing that information?

Mr BLUEMMEL: Yes. In short, it does not, and the reason for that is that the handling of information for which we are responsible is the handling by state and local government agencies. So, I mean, if the information got out there because of a breach by a state or local government agency, then, yes, we would be very interested, but if it is just someone who has done their own little bit of digging and then publishes it in an amateur journalist way, generally speaking that would not be something of our concern.

Mr GRIMLEY: I thought so.

Ms DIXON: One of the things that you might want to consider there, though, is whether or not that information being publicly available should be available to government to use, and I think we would make the argument there that no, it probably should not. Government has a higher responsibility to do less harm, I would suggest. One of the issues in privacy, I guess, is that one of the exceptions in some privacy Acts can be if information is already public. Obviously there are situations where information is leaked to the public, but you do not want it to continue to be leaked. Now, you can never take information off the internet—it tends to persist indefinitely—but the degree to which you can do less harm by not resharing that information I think is something that you probably do want to protect.

Mr GRIMLEY: There have been a number of times, as an ex-member, where I have been contacted as a sexual offences detective by people saying, 'Mr X is living wherever. I saw him and his photograph on the internet, on this particular website'. So therefore then it is up to the police to begin that investigation to see if there is any risk to the public. So there is a line that is being blurred there at times with accessing that information, using that information and conducting an investigation, and of course not releasing official information back to that person or complainant. I am just making you aware of that. It might come across your desk at some stage—not me, but somebody else.

Now, can I just ask you a question about the unintended consequences that you spoke about in relation to vigilantism and a false sense of security or the inference to a false sense of security? Are you able to elaborate on that at all in terms of any evidence or research that you can direct the committee to, to go over?

Mr BLUEMMEL: Look, nothing that is not already in submissions before you, I think. I know that I think in Western Australia there is one prosecution for unauthorised use—

Mr GRIMLEY: Three.

Mr BLUEMMEL: Three, was it? But really in addition to what is already there in submissions, I am not aware of anything beyond that.

Mr GRIMLEY: There were 390 000-odd times that their website was accessed, and I think three times a person has been charged, which is quite small in the scheme of things. I was just interested to know: the false sense of security, I have heard it before and I have asked submitters also where the evidence comes from for that, and no-one has been able to assist.

Mr BLUEMMEL: I think for us where we drew that from was looking at some of the other submissions you have in terms of what proportion of sex offenders information would actually end up being on a register by virtue of lower reporting rates, low prosecution rates and so on. So that to us was a factor, because if it is a small proportion or even a very small proportion, then clearly the idea that there are other sex offenders out there who are not on the register, I think would be deducible from that.

The CHAIR: Sheena, are you fine?

Ms WATT: Yes, I really am. Thank you so very much.

The CHAIR: Tien?

Dr KIEU: Thank you. Something that has come to my mind, and this is quite recent, so maybe OVIC can answer or maybe someone can inform me. My question is related to the Spent Convictions Bill that has been passed by the Parliament recently. These will be automatically spent for children who are even convicted of sexual offences. So the first part of the question, to clarify, is: would those young offenders be on the register as a sex offender if it was committed against another child; and if it is the case, then when the conviction is expunged or spent, what happens to the register?

Mr BLUEMMEL: I am not sure of either of those, I confess, either in the current state or what it might do for any future greater access to the register. I am not familiar enough with the legislation behind the current scheme, I am afraid. I could not give you an informed answer.

Dr KIEU: No, no. I understand that this is very recent, so something that I myself should look into. It is just because at the moment you see people, inactive people, still being maintained on the register, so I am just

wondering what would happen to people who have a spent conviction. But anyway, that is my worry. Thank you.

The CHAIR: Thank you. Ed, you have no further questions.

Mr O'DONOHUE: No, thank you.

Mr GRIMLEY: Just one more if I can.

The CHAIR: Yes, of course you can.

Mr GRIMLEY: Just going back to what Dr Kieu was saying, I think children are exempt from what he is talking about. I believe it, but I will clarify that. My question is just in relation to the Western Australian model that we have been speaking about. If a similar scheme were to be implemented in Victoria, do you believe the release of information should be centrally managed and dealt with or would it be more suitable on a local level?

Mr BLUEMMEL: I do not know to what extent the Western Australian model has done that. I think it is central there, but I am not sure. I think the benefit of doing it centrally would be that there would hopefully be a consistent approach and also that the operators of the system would be able to notice trends, level of demand and so on. And if there is a restricted model of access where only certain individuals after proving their location or anything like that would have access, then I would think that a central system would make it harder for a person who should not have access to mislead different parts of an organisation into giving them access. Those are just some thoughts off the top of my head.

Mr GRIMLEY: And can you tell me: do you know if there is a similar OVIC in Western Australia at all?

Mr BLUEMMEL: The situation in Western Australia is a bit different. There is an Office of the Information Commissioner—it is an office I used to hold some years ago—but the remit of that office is purely freedom of information. There is no current privacy legislation that applies to state and local government in Western Australia there. They are one of only two jurisdictions. The other one is South Australia. And so certainly the commonwealth *Privacy Act* applies to businesses above a certain size in Western Australia as well as to commonwealth government entities in Western Australia, but there is no privacy legislation that applies to state or local government in Western Australia at all. So for the purposes I think of that question the answer would be no, there is no privacy regulator as such.

Mr GRIMLEY: Thank you. Thanks, Chair.

The CHAIR: Great. Thank you both very much for again appearing before this committee and for providing your detailed and in-depth knowledge in this area. As I mentioned, a transcript will be sent to you in the coming days, so please do look at that and make sure that we have not incorrectly represented you. Thank you again.

Witnesses withdrew.