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, 13 May 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

WITNESS

Dr Craig Horne.

The ACTING CHAIR (Ms Garrett): We are delighted to have you here, Dr Horne. I am just going to give you some information around your evidence here today. All evidence taken is protected by parliamentary privilege as provided by the *Constitution Act 1975* and further subject to the provisions of the Legislative Council standing orders. Therefore any information you provide during the hearing is protected by law. You are protected against any action for what you say during this hearing, but if you go elsewhere and repeat the same things, those comments may not be protected by such privilege. Any deliberately false evidence or misleading of the committee may be considered a contempt of Parliament.

All evidence is being recorded. You will be provided with a proof version of the transcript following the hearing. Transcripts will ultimately be made public and posted on the committee's website.

For the Hansard record, could you please state your name and any organisation you are appearing on behalf of.

Dr HORNE: My name is Dr Craig Horne, and I am the Managing Director of Informational Risk Pty Ltd.

The ACTING CHAIR: Thank you very much. We welcome your opening comments but ask they be kept to a maximum of 5 to 10 minutes to ensure we have plenty of time for discussion. Thanks, Dr Horne.

Dr HORNE: I do not have any slides. I have just got a short, prepared speech. I have not timed it, but it is only three pages so hopefully we will rip through that.

Dear members of the board of Inquiry into Management of Child Sex Offender Information. Thank you for the opportunity to present here today. I hope to offer further insight into child sex offender information management, building upon my original submission.

A little bit about myself, I would like to begin by describing what I am not. I am not a child sex offender expert. I am not an expert in victim justice or offender recidivism. I am not a psychologist nor an expert on motivational desires to commit child sex offences. I am not an expert in policing techniques or punishments for offenders. What I am is an information security expert. I completed a PhD on information security strategy at the University of Melbourne, where I conducted research into understanding how leaders of an organisation might make decisions to use their information sustainably towards the achievement of goals. This research gives me insight into the most appropriate ways to manage high-sensitivity information. Also, to some extent I might be considered a technology expert as I have a Bachelor of Science majoring in computer science and an MBA majoring in management information systems, so I think I am qualified to advise whether information should remain confidential or otherwise and why.

To recap my initial submission, I am in support of the public disclosure of child sex offender details, which I will refer to as 'the proposal' from now on. I argue that there is a strong body of evidence to show that deterrence is a reliable and effective countermeasure to crime. For a deterrent to be effective in controlling the behaviour of rational people, it must be swift, severe and certain. To expand, deterrence theory states that formal sanctions such as custodial sentences imposed by the courts ensure that potential offenders consider both the risks and the costs of their intended illegal activity before they engage in it. Informal sanctions such as public disapproval also affect potential offenders.

In relation to the proposal for child sex offender identities to be disclosed in a public register, this sanction should be imposed immediately upon verdict, which makes it swift, published in every newspaper in the country, which makes it severe, and unable to be overturned on appeal, which makes it certain. The impacts of child predation on citizens in the state of Victoria can be varied and powerful. For example, the police resources required to investigate, the court costs to prosecute, the financial costs of decades of incarceration and the lifelong impacts on the victim and their loved ones are profound. The impacts on the predator are also profound. For example, a rational offender will forever have to live with shame plus a conviction and will therefore find it difficult to find any employment that requires a police check. On balance, however, the Victorian public interest should override the interests of the offenders.

Since being invited to present here today I have thought more deeply on this topic. We need to clarify what our goal is. Without agreeing on a goal, we will always disagree on a path going forward because we are going in different directions towards different goals. I assume that the goal of this proposal is to protect children. To put the topic of this in security terms, the asset being secured is children. I am assuming for the purposes of this inquiry that all Victorian children are equally high value and that we want to protect them all. This is different to how I view assets in my day job, where information being used as an asset can be high or low value, the implication being that low value information assets would have fewer controls applied to secure them, which saves money. In this scenario, given children are high-value assets, we want to apply the maximum level of security controls that we can. A sex offender is a threat, and this idea to publicly disclose a sex offender's identity is a security control in the middle keeping them apart.

Most threats are already known, and by publicly identifying a sex offender we are helping to increase the preparedness of other institutions that have to safeguard children, such as families, schools, childcare centres, child leisure activity centres or anywhere that has a responsibility to protect children. These institutions have different resources at their disposal. For example, families would typically have less money than schools. Where a school has the resources to run a police check on a prospective teacher, a family may not have the resources to run a police check on a prospective nanny. However, by publicly identifying sex offenders the playing field levels up and a family can run a simple Google search or register inquiry to help them make the best decision.

It has become clear to me that there are two benefits to this proposal, not just one. I have already identified that this proposal acts as a deterrent for future offenders, which reduces known and unknown threats. It also helps institutions that are charged with protecting children to prepare, which increases controls. Threats can be known or unknown. Known threats can and should be protected against, and this proposal to publicly disclose the identity of sex offenders to deter offenders is a good example of how to deal with known threats. Of course there are unknown threats as well, where past offenders have not been caught yet or potential offenders have not acted yet. An important property of threats is that they can change and be more focused or be degraded either by eliminating the threat completely or by degrading their motivation, resources or capabilities.

Similarly, security controls can change. Security controls are defined as an appropriate mix of physical, technical or operational countermeasures to threats. The goal of controls is to mitigate the risks to assets. Controls are used to protect assets by reducing the risk posed by exposures or vulnerabilities arising from threats. Controls are most effective when they are applied in proportion to the value of the asset being secured or degree of threat to the asset, so it is important to realise that control effectiveness can change up and down. It is important to understand that this proposal is just one security control, albeit an important one. Many controls should be put in place that overlap to create defence in depth to protect Victorian children.

I have already argued that I think the child sex offender register should be made public, but I want to clarify scope and say that I do not think that the names of juvenile offenders should be made public. Whilst I accept that some children are born psychopathic, lacking the human trait of remorse—as in the tragic case of 10-year-old Robert Thompson and 10-year-old Jon Venables murdering two-year-old James Patrick Bulger in the UK in 1993—other children may have well-developed values but end up on the register for a singular error in judgement. Given childhood is a confusing time for most children while they are learning the rules of society and it is possible they might completely rehabilitate but it would be too hard to distinguish between the two cohorts, all children's names on the register should not be made public, if we define a child as being under 18 years old.

Another consideration is whether this countermeasure should be retrospective to include sex offenders previously registered or whether it should only act as a deterrent for possible future offenders. My view is that this countermeasure should be retrospective. However, it should only apply to people who are still alive and therefore could still be a threat. Offender age and any previous rehabilitation should not affect this decision because the integrity of the offender is non-existent. I often say that integrity is like a balloon: it is either there floating in the air or you pop it and it is gone—you cannot have half-integrity. So sex offenders have no integrity when it comes to deciding whether they will offend again.

There are risks with this approach of course. These risks include hackers changing the name of someone in the online register or adding a new name, vigilantes attacking a sex offender or their family members and increased cost to the public purse if an offender cannot work after the public disclosure and needs to be supported financially by the state. My view is that each of these risks can be mitigated with an appropriate control.

If government does decide to proceed with publicly disclosing sex offender details, then I have some suggestions, which are: one, sex offenders on the register are banned from ever changing their name; two, if that is not possible, then when a sex offender on the register does want to change their name they are required to apply beforehand and notify afterwards where this has occurred and the register should be updated with the new name; and three, the public disclosure of sex offenders on the register is limited to those aged 18 or older.

To conclude, I am in support of the full public disclosure of Victorian child sex offender details. I think it is a logical and prudent step to take in preventing future insidious attacks against the greatest asset the state of Victoria has, -children- who are our future. Thank you for this opportunity to contribute today, and I am happy to take questions.

The ACTING CHAIR: Thanks very much, Dr Horne. That was a very comprehensive presentation, and we appreciate it. Does anybody want to kick off? Ms Watt, did you have any questions?

Ms WATT: I might need a moment, Chair, if that is all right.

The ACTING CHAIR: That is fine, no problem at all. Mr Grimley.

Mr GRIMLEY: Thanks, Chair. Thanks, Doctor, for your presentation. And I totally agree that our goal should be about protecting children, absolutely. You suggested that there is a strong body of evidence to show that deterrence is reliable and effective. Can you just expand on that and perhaps direct the committee towards some evidence to support that statement?

Dr HORNE: Yes, absolutely. A deterrent needs to have three properties: swift, severe and certain. If it is missing those, then it lacks its deterrent effect. So when you see cases in court where appeals overturn original convictions and that kind of thing, it leads to people thinking, 'Well, I can probably get away with this, or if I can't, I'll overturn it later. It's not a permanent mark', you know? The severity is important to instil fear in the potential offender and change their actions when they are weighing up the risks or the costs for their intended actions. I did include some references in the original submission that expand on that in much more eloquent terms, but effectively those are the three criteria that need to be met to make a deterrent effective.

Mr GRIMLEY: I have got a journal article here that was supplied also, 'A review and analysis of deterrence theory in the IS security literature'. Is that one of the references you are referring to?

Dr HORNE: Yes.

Mr GRIMLEY: Did you want to speak about that at all in broad terms? What is deterrence theory in particular? What is that about?

Dr HORNE: From our perspective what we do is we consider threats, both external and internal, to an organisation, because insider threat is just as insidious as the external threats. Once an organisation is connected to the internet, then you open up the door effectively to the entire world of hackers, globally. Any hacker can potentially circumvent controls and enter a company's network and start to access information.

I am on the business side of information security, and so we try and understand the human psychological aspects to it and best ways to manage information systems. There are a lot of aspects to information security on the people side if you consider how an organisation would govern—effectively your job—and how would you govern the controls that are put in place to protect the children of Victoria. Risk management policies, what policies would you set; the strategy for going forward; your accountability if you get a decision wrong; the culture that we create out in the community; and security education and training awareness programs all help combine and I think all are necessary to create a holistic approach to securing information. And you can measure your maturity in each of those discrete areas. So if you run a maturity assessment and you come across an area that is not that strong, you simply identify it, resource it appropriately and put it on the road map for the next 12 months to improve.

So deterrence is a way to both—what you are trying to do is degrade the threat's capability, both internal and external, to an organisation, by making them aware, increasing the chances they will get caught and that the punishments, if they do get caught, are quite severe—swift, severe and certain. Does that make sense?

Mr GRIMLEY: Yes. Thank you, Chair.

The ACTING CHAIR: Thanks, Mr Grimley. Mr O'Donohue, do you have any questions?

Mr O'DONOHUE: Thanks, Chair. Look, I do not have any questions at this stage, but thank you very much for the submission. It has been most helpful.

The ACTING CHAIR: Ms Maxwell.

Ms MAXWELL: I am happy to defer any further questions from me to Mr Grimley. Thank you, Acting Chair.

The ACTING CHAIR: Ms Watt.

Ms WATT: Hi. Thank you, Dr Horne, and thank you, Mr Grimley, for giving me a moment to gather my thoughts. Can I thank you for your contribution today and for your submission. I am interested in understanding more about the deterrence theory, which you have spoken about a couple of times now, and I must confess it is a new one for me. I wonder if you could talk more about the body of evidence around this deterrence theory—where it comes from and what the sort of background evidence is around that—because it is certainly worth further consideration. Thank you.

Dr HORNE: Yes, absolutely. It sounds like that is a common question. Would the inquiry like me to put together some more information into a further report or something and send that through?

The ACTING CHAIR: I think that would be very helpful. I think this is an area of exploration for us that we would be interested in. So yes, if you could, that would be terrific.

Dr HORNE: Yes, okay. No worries. And if I can put together a more considered response to your important question, I guess at the end of the day that is the whole point of this, isn't it? Publicly disclosing their details is deterring future offenders.

Ms WATT: Yes, I certainly would appreciate that, and thank you, Acting Chair, for that. I am happy to perhaps pass to another questioner and return to me if there is an opportunity, Acting Chair.

The ACTING CHAIR: Does anyone have any further questions?

Mr GRIMLEY: Thanks, Chair, if I may.

The ACTING CHAIR: Mr Grimley, you are back.

Mr GRIMLEY: Is that okay? I am here; I have not left. You spoke about risk factors to assets, in particular hackers. Are you able to sort of elaborate on that or provide any evidence of this risk factor, of hackers being an issue at all, in particular within Victoria, of accessing confidential information?

Dr HORNE: Yes. So what is your question exactly? What would you like to know?

Mr GRIMLEY: So you mentioned that hackers were a potential risk factor to the asset. I am just interested to know if you have any experience or evidence about that being a live issue or a previous issue within Australia, Victoria or international jurisdictions. When it comes to the storage of confidential information and the releasing of that information, how has that been manipulated in the past by people outside organisations?

Dr HORNE: Yes, sure. There have been a few instances recently in Victoria of hospitals having their systems compromised and patient records being accessed. That is deeply personal information, and if someone has caught a particular disease, I am sure their insurance company would want to know about that or their employer, or their friendship circles if there is some stigma attached to the disease. There is a real issue around keeping that information confidential.

To bring that back within the context of this inquiry, there are a couple of approaches to securing this information. One is that we lower the value of the information or we increase the controls. What I mean by that, just to expand on that a little bit, if you are going to put together a register of information and make it publicly available, make that register isolated: just have the information in it so that if it was hacked, you would be comfortable with it being out there because you have already publicly disclosed it. But you do not want to have an entire offender's details on this website and then just disclose a few of the fields in that record in case

someone does get access to the website and they get access to the entire record, if that makes sense. Just put the details that you want to disclose in a database on the website, and so if it does get hacked, they do not get access to anything else. It is called devaluation, where you are compartmentalising and devaluing the information that you are holding in that receptacle.

The other idea is to increase your controls. So for something like this integrity remains important. If two neighbours are having a dispute, you would not want one putting the name of his neighbour into this register to try and create a furore. You would charge the department with applying the maximum levels of security controls available in the world to protect that information and ensure its integrity, even though the confidentiality of the information is not going to be an issue. It is a bit like a sales brochure or a website; they are examples of information that you do want public. A sales brochure you want everyone in the world to read, it is not something you want to keep confidential, but you still want to maintain the integrity of that. Especially websites—you would not want them defaced with pornography or other terrible things, you want to just have a sales approach to it. Similarly here you would want to make sure just the offenders' details were in that database.

Mr GRIMLEY: Do you have any experience with the Western Australian disclosure model at all, of the sex offender information?

Dr HORNE: No. I do not.

Mr GRIMLEY: No? That is okay. I just thought I would cross that off. Just one more question if I can, Chair.

The ACTING CHAIR: Absolutely.

Mr GRIMLEY: What safeguards and protections do you think would be necessary to ensure that the information contained in a public register is used appropriately for those that access it? You mentioned the devaluation of the details—

Dr HORNE: Of other details, like the home address of the offender and stuff like that.

Mr GRIMLEY: Yes. Would there be anything else that you think we would need to consider in terms of safeguards or protection of that information?

Dr HORNE: If I can expand a little bit, there can be nuanced levels to this disclosure of information. You might decide to not make it fully public, but you might decide to share it with every single law enforcement agency in the world—all over Australia and all over the world, every other country—so that person, if they do travel overseas, will get tracked or that other country has the right to refuse entry and all sorts of things like that. Or you might make it fully public so that mums and dads can protect their children against someone applying for a job as a nanny or if they have some other close contact with children.

I am not sure if you are aware that the department of justice have a lot of prisoner records—they are experts in this, and you should have someone come in and speak to you from the department of justice, because they have got a lot of experience with that—but they hate going online with prisoner records. They still have pieces of paper and folders for prisoners, because they cannot get hacked. That is devaluation. That is separating the threat from the asset. There is no physical connection; there is no way it can get hacked. That would be the approach you would take with a website. If you did put a register in a database on a publicly available website, just put the details in there, you would design the database not to have multiple fields. It would just have first name, last name—that is it.

The ACTING CHAIR: Thank you. Mr Grimley, do you have further questions?

Mr GRIMLEY: No. Thank you, Chair.

The ACTING CHAIR: I cannot see anybody else with further questions. Yes. I have got no communication there. I very much appreciate it, Dr Horne. It has been very interesting for us, and we look forward to that further information that you are going to provide around deterrence theory. I wish you a good day.

Dr HORNE: Thank you very much, Madam Chair. Hopefully I have added a different viewpoint.

Mr GRIMLEY: Great. You did. It has been very interesting.

Witness withdrew.