TRANSCRIPT

INTEGRITY AND OVERSIGHT COMMITTEE

Inquiry into the Education and Prevention Functions of Victoria's Integrity Agencies

Melbourne—Monday, 7 June 2021

(via videoconference)

MEMBERS

Mr Stephen McGhie—Chair	Ms Harriet Shing
Mr Brad Rowswell—Deputy Chair	Mr Jackson Taylor
Mr Stuart Grimley	Hon Kim Wells
Mr Dustin Halse	

WITNESSES

Dr Suelette Dreyfus, and

Dr Chris Culnane.

The CHAIR: I declare open the public hearing for the Inquiry into the Education and Prevention Functions of Victoria's Integrity Agencies. I would like to welcome any members of the public watching the live broadcast. I also acknowledge my colleagues participating today and those that are an apology for this session.

I would like to begin this hearing by respectfully acknowledging the Aboriginal peoples, the traditional custodians of the various lands each of us has gathered on today, and pay my respects to their ancestors, elders and families.

All evidence taken by this Committee is protected by parliamentary privilege. You are protected against any action for what you say here today, but if you repeat the same things anywhere else, including on social media, those comments will not be protected by this privilege. Any deliberately false evidence or misleading of the Committee may be considered a contempt of Parliament.

All evidence given today is being recorded by Hansard. You will be provided with a proof version of the transcript for you to check as soon as available. Verified transcripts will be placed on the Committee's website. Broadcasting or recording of this hearing by anyone other than Hansard is not permitted. I remind those that are involved in this Zoom meeting today to please mute your microphones when not speaking and please switch your mobile phones to silent.

I welcome Dr Suelette Dreyfus and Dr Chris Culnane today to do a presentation. Suelette is from the University of Melbourne's School of Computing and Information Systems, and Dr Culnane is an independent cybersecurity and privacy consultant and former lecturer at the University of Melbourne. We welcome your opening comments for 5 to 10 minutes, which will be followed by questions from the Committee members. I will hand over to you, Dr Suelette and Dr Chris, to introduce yourselves and then provide us with an opening address. Over to you. Thank you very much.

Dr CULNANE: Thank you. I am Dr Chris Culnane. I am an independent cybersecurity researcher, as mentioned, and I previously was at the University of Melbourne and continue to have an honorary position there. Thank you for the opportunity to appear before you today. Our submission covers two aspects of the education and prevention functions of Victoria's integrity agencies. Firstly, we briefly discussed whether the current oversight of access to health data by the Health Complaints Commissioner instead of the Office of the Victorian Information Commissioner creates duplication and divergence from the best practice offered by OVIC. Second, and the bulk of our submission, is whether the educational material and support provided by IBAC to facilitate anonymous submissions to public interest disclosure coordinators are both sufficient and technically consistent.

With regard to the first issue of oversight of health data, it is our view that it would be better delivered were responsibility to lie with OVIC. OVIC has for some time been at the forefront of Australian privacy regulators in providing educational material and guides for the protection of data. They have demonstrated an effectiveness in providing explainers on complex topics as well as detailed and informative investigations where breaches have occurred. This is in marked contrast with the Health Complaints Commissioner, which has scant information about the challenges and methods of protecting health data. Health data is some of the most sensitive data that can be held or processed, but fundamentally the techniques for protecting it are no different; there is just a greater importance to get them right. As such, for consistency in both education definitions and guidance, a single point of reference for the protection of data is desirable.

With regard to the second issue and the bulk of our submission, we have raised a number of questions about the consistency and effectiveness of the education and support material provided by IBAC. Facilitating effective and safe public disclosure has two core requirements. Firstly, the systems deployed must be technically sound and deliver the promised security and anonymity properties. Second, the educational materials provided to encourage disclosure must be consistent with the properties that have been delivered. Divergence between those two requirements creates a risk that could undermine the entire scheme. Were a breach of anonymity to occur in a situation where a discloser had been promised such anonymity, it could destroy trust in the scheme as a whole and suppress future disclosers.

Current IBAC education material makes strong claims on anonymity, yet the equivalent guidance and practical advice for the public interest disclosure coordinators lack the rigour and detail to expect such anonymity to be achieved. We raised particular examples with regard to email submissions and the lack of specific advice to the discloser. More broadly, the challenge of anonymous disclosure is a hard one, particularly in an environment in which cybersecurity technologies are increasingly invasive. The guidance provided to those responsible for setting up such an anonymous disclosure system is somewhat lacking and does not take advantage of replicating best practice from elsewhere in the world or even between different organisations. We recommend a more hands-on approach to the provision of such services, including the provision of centralised managed services for secure drop boxes to allow public interest disclosure coordinators to focus on the task at hand—handling disclosures—and not on the challenges of deploying technology solutions.

I will now hand over to Suelette, who will make some further opening comments.

Dr DREYFUS: Thank you very much, Chris. Thank you very much for having me here today and inviting me to speak. I am delighted to be here, and I would like to acknowledge that this is being held on the traditional lands of the Wurundjeri people of the Kulin nation and pay my respects to elders past, present and future.

I am a Senior Lecturer, as you said, in the School of Computing and Information Systems at the University of Melbourne, but I speak as someone who has expertise in the topics covered today as myself, not as a spokesperson for the University. I have studied and written about whistleblowing in particular. Obviously whistleblowing is a crucial part of anti-corruption activities. Prior to earning my PhD and going into academia I worked as an investigative journalist, so I know about whistleblowing on many different levels. Clearly whistleblowers are very important to the integrity agencies being able to do their job, and how the agencies communicate with whistleblowers is crucial, as is educating the public about whistleblowing, because doing so well helps prevent corruption. In this way what I speak about today addresses the education and prevention functions of the integrity agencies.

Firstly, we say that any critique we may give of the agencies involved is against a backdrop of technology and social change disrupting business-as-usual in the anti-corruption space. This is important, particularly in our COVID-induced isolation, and my comments are meant to enlighten and improve, not to accuse. Secondly, I would like to give some context. Currently I have spent a fair bit of time studying the use of secure drop boxes in Europe as an anti-corruption measure, among other things, and whistleblowing more generally. To give you a bigger sort of worldwide picture, Europe is leading the way in the pace of change of whistleblower protection reform, and this is a major anti-corruption push. This reform is driven by the EU [European Union] directive covering whistleblowing protection which was passed in the European Parliament in Strasbourg in April 2019. It was a pretty momentous moment for many in civil society and academia who had worked four or more years to bring this change in, and I myself was a part of that change and very pleased by it.

The directive requires 27 countries to pass national laws protecting whistleblowers by the end of this year, 2021. Let me just say that again: 27 countries. Other countries globally are following suit, and Europe has been gearing up for how to address this momentous change. Secure drop boxes and channels to anti-corruption agencies are a part of that. Technology to enhance whistleblower protection and support anti-corruption efforts is most definitely playing a key role in it. It is not only in Europe; Mexico is currently in the process of working with academic experts and civil society to draft its first whistleblower protection law. The initial draft, which is not yet made public, includes state-of-the-art technology requirements embedded in it. When Italy passed its substantive whistleblower protection law in November 2017 it specified companies use ‘technology capable of ensuring confidentiality of the whistleblower’s identity’—of those making disclosures—and is believed to be the first legislation in the world to do so.

Agencies who are covered in this review today are an important avenue for whistleblowers. They need to be thinking about this change in technology and how it is going to change and disrupt the landscape. Every agency, in my view, should offer technologically secure—genuinely secure—digital drop boxes for disclosures, and those should all offer anonymous channels. It is important for public outreach and education as well as developing trust. Secure drop boxes are spreading worldwide, not just in anti-corruption agencies. There are more than 100 secure drop boxes in use around the globe today in civil society, government, and media organisations. That does not even count the private sector. So that does not count companies that do compliance work, for example. Spain is a leader in this field. The anti-corruption agencies of Valencia, Catalonia and Barcelona all provide these boxes with anonymity options. It is not enforced on the end user but it is given as a choice.

Public authorities who have implemented secure online drop boxes have generally found them to be of significant value, and that is also true of NGOs that fight corruption who offer these secure channels. For example, Transparency International Italy channels all its public enquiries through its GlobaLeaks instance—GlobaLeaks being one of the secure channel providers that is on offer—and that makes it possible to have anonymous communications explicit for anyone who wants to get in touch with them to make a disclosure.

Some colleagues of mine working on a report that I also worked on interviewed someone from BaFin, the German financial regulator, and they have been running an instance since 2017 and they talked very much about the benefits of anonymous reporting schemes far outweighing any disadvantages. In fact they said, quote, 'It's important that this option exists because it enables whistleblowers to submit their information to us without exposing themselves to unnecessary danger. We highly value the possibility of anonymous reporting'. In addition, I believe we would not receive the majority of the reports we are now getting if we did not have the opportunity to do this anonymously. They do raise, however, the importance of having a well-defined legal framework—and this is something that Germany has been identified as needing to work on—which provides a kind of insurance for officers who are handling these anonymous reports, and that is something that Victoria should be thinking about.

In a broader picture, anonymity is a kind of privacy. That is how I define it when I teach in this space. We know that whistleblowers face reprisal, and the decision or not of whether to reveal one's identity really should be left to the individual whistleblower because of the risk of reprisal. Now, that is pretty consistent with a government policy that focuses more broadly on disclosure, not on the person making the disclosure—and, after all, the whole point is to stop wrongdoing, not to shoot the messenger.

If I were to make a few kind of key conclusions about what Victoria should be looking to in the future to be a leader on this globally—and I think it can be—it is for every agency in this space covered by this review to be asking itself, 'Do we have an effective anonymous drop box, a digitally secure drop box, that people can go to from the website and use with safety and anonymity, that has been tested externally as being so, and are we offering these dual channels for whistleblowers in a way that is communicated clearly, that there is a dual channel? Is there an avenue for follow-up communications from the submitter that allows live chat—and by that I mean typing; it does not necessarily have to be voice—'that offers both security and the option of anonymity to the agency?' A live typing chat session is ideal, but it also should have, for example, file transfer capability that is also anonymous. Personally I recommend open-source technology that has been reviewed by the broader community, because I think that this will instil more confidence and trust from the community.

A third point is to get all of these services externally tested and also tested from a user-experience perspective—an independent, arms-length user-experience perspective. The result of those tests, particularly security tests, should be made public and there should be an explanation of how any flaws have been fixed—again, for public trust—and this is done routinely with security software that is made open source to thecommunity, and people are much more confident using it as a result.

Fourth, a clear explanation of all the above to the public who want to make a submission, in plain English. Sometimes using an anonymous channel, as opposed to a secure but non-anonymous channel, can be a more complex thing to do. So the public needs to be able to understand very clearly what those trade-offs are in simple terms.

Fifth, statistical data should be released to the public annually for the use of these avenues—and particularly about the technology wherever possible. It is important for researchers to have it. It needs to be done in a way that protects privacy, and people such as Dr Culnane, Professor Ben Rubinstein and Associate Professor Vanessa Teague are all recognised international experts in this space and I am sure would be happy to assist any of the agencies in doing so in a way that protects privacy.

Among whistleblowers, there is a concern that agencies may sometimes simply provide avenues that, and I quote specifically from a whistleblower, may just be 'dead-end labyrinths by design'. Dead-end labyrinths by design. This is how a Commonwealth whistleblower described to me their view of the channels that were offered. That is clearly not success, and that sends a message to other whistleblowers: don't step forward, don't make a disclosure, don't reveal corruption. So it is very important that that is not what actually happens in Victoria. This is really in a sense the highest-level objective—to avoid that—because if you really want a system that enjoys public trust, you have to have good technology well communicated, and then from that you will get trust and hopefully good anti-corruption disclosures. Thank you.

The CHAIR: Thank you, Dr Suelette Dreyfus and Dr Chris Culnane. Thank you very much for that presentation. I will open it up to Committee members for any questions.

Mr ROWSWELL: Thanks, Chair. Thank you, Dr Dreyfus, and thank you, Dr Culnane, for your presentations. For you to be proposing what you are proposing in a very detailed and comprehensive way, as you have, you must have drawn the conclusion that the existing anonymous disclosure framework that operates within Victoria is flawed or needs significant expansion or improvement. Is that a fair assessment?

Dr DREYFUS: Do you want to take that one, Chris?

Dr CULNANE: I think it is primarily looking at the technical advice and guidance that is being provided. We see there is a high technical challenge in delivering anonymous whistleblowing and anonymous drop boxes, and so typically we would expect to see an equivalent level of either technical guidance or explicit provision of services. Where we do not see that we do not expect that someone would achieve anonymous disclosure without having gone to some fairly extreme lengths to do it in that it is a significant technical challenge, and so because we are not seeing that aspect of it—and some of the inconsistencies around, for example, suggestions of using email as an anonymous way of doing the disclosure—our concern is that there is a slight disconnect between the technical provision and the desire. So there definitely is the desire to have an anonymous disclosure pathway, but we are not seeing the provision of the technical side.

Mr ROWSWELL: Thank you, Chair.

The CHAIR: Any other questions? No. I have just got one question. If Europe is leading the way with anti-corruption—and I know, Suelette, you referred to the three or four things before about anonymous drop box and dual channels and following the communication—I mean, what are the learnings for us? And why would we be so far behind?

Dr DREYFUS: I do not think it is through any lack of will. Europe is absolutely on a learning curve, and there are plenty of places in Europe and elsewhere that are not necessarily heading in the right direction. In fact Dr Culnane and I were just speaking yesterday about Canada's anti-fraud agency, which is on a path to have people having to register to make a submission, which is the antithesis of anonymity really. So it is not universal across Europe, but I think the thing that has made the big difference is that the EU directive on whistleblower protection is coming hell or high water. So this was passed by Strasbourg, and a lot of the governments of the 27 countries are not happy about having to implement this, but they have to do it; it is legally binding. And by virtue of that there has been a kind of a slow-build groundswell within governments. They have slowly realised it and they are starting to change, as well as the private sector. So one thing I have taken great heart from is that the private sector—and I am all for this; I think it is great—has finally realised that there is some good business to be had in doing this properly, and they are getting out there with new products to offer companies, small and medium-sized companies as well, how to set up these secure channels. I think that industry is fairly nascent in Victoria for, say, medium-sized businesses. It is sort of handled pretty well at the top end of town.

So that change in legislation has been a big push in Europe, and that is a good thing, but what I see is that some resourcing for our anti-corruption agencies to actually learn from Europe would be a potentially very good thing. Even just a small, informal network that would allow them to liaise with the very friendly and willing-to-be-helpful people at the anti-fraud agency in Valencia, for example, or in Catalonia would be a terrific thing because they can kind of troubleshoot. So I think those sorts of things would be most helpful. Also perhaps a landscape—a sort of environment scan, if you will—of the options that are available, particularly in the open-source sector for institutions, would be a good thing as well, and potentially some independent review of that, some independent testing of that, would be helpful too. So I suspect it is partially our isolation, maybe some language barrier, not necessarily facing new legislation in exactly the same way Europe has—the combination of those things. And if we can find ways to support that kind of oil the wheel a little bit to turn faster, then it might help push things along. Does that explain it?

The CHAIR: Yes, it does. Thank you for that. I appreciate that. Mr Rowswell.

Mr ROWSWELL: Just a very brief question. Just to finish off on your last point there, who do you think should take responsibility within government to oil the wheel? What is the agency that is most appropriate to advance this, should it be determined within government that it is a worthy thing to advance, and I think it is. Who is the responsible agency?

Dr DREYFUS: It is actually an interesting question. I would have to think about whether or not it made sense to do that centrally or whether to do it in each agency. Sometimes a somewhat decentralised approach to implementation can be helpful, because peers kind of learn from each other and leapfrog over problems that ‘my mate down the road had—so I do not repeat that problem’. But I think Chris might have a view on that as well. If you wanted to jump in on that, Chris—

Mr ROWSWELL: I am happy for you to take it on notice as well.

Dr DREYFUS: Yes.

Mr ROWSWELL: There is no need to come with the answers now. But if you are happy to take it on notice and give it consideration, perhaps the both of you, and come back to us, then we are happy with that too.

Dr DREYFUS: Yes, I think that would make sense. Chris, do you have any thoughts?

Dr CULNANE: Clearly if we take that on notice, we will give a more detailed answer.

The CHAIR: Great, that is great. Thanks, Mr Rowswell. If there are no further questions, I just want to extend our appreciation for your presentations today. And I believe, Chris, you are in Sussex at the moment and it has just gone past 8 in the morning, so thank you for getting up early and participating in today’s hearings. I really appreciate that. As the Deputy Chair, Mr Rowswell, has just indicated, there may be some questions on notice that we would like to put to you. If there are, we will do that as soon as we can and we will get those questions to you for you to consider and respond to.

I just want to extend our appreciation for your submission and your presentation today and for answering the questions of all of our Committee members today. We really appreciate that. On that basis, I would declare this public hearing closed.

Committee adjourned.