T R A N S C R I P T

LEGISLATIVE ASSEMBLY LEGAL AND SOCIAL ISSUES COMMITTEE

Inquiry into Anti-Vilification Protections

Melbourne—Thursday, 28 May 2020

MEMBERS

Ms Natalie Suleyman—Chair
Mr James Newbury—Deputy Chair
Ms Christine Couzens
Ms Emma Kealy
Ms Michaela Settle
Mr David Southwick
Mr Meng Heang Tak

WITNESSES

Professor Lyria Bennett Moses, Director and

Mr Siddharth Narrain Arcot Ananth, PhD candidate and Scientia scholar at UNSW Law, The Allens Hub for Technology, Law and Innovation (*both via videoconference*).

The CHAIR: Welcome to the Legislative Assembly's Legal and Social Issues Committee public hearing into anti-vilification protections. I would like to begin by acknowledging the traditional owners of the land on which we are meeting here today. I pay my respects to their elders past, present and Aboriginal elders of other communities that may be here today. All evidence taken at this hearing is protected by parliamentary privilege as provided by the *Constitution Act 1975* and further subject to the provisions of the Legislative Assembly's standing orders. Therefore the information you provide during the hearing is protected by law. However, any comment repeated outside the hearing may not be protected. Also, any deliberately false evidence or misleading evidence to the committee may be considered a contempt of Parliament. All evidence is being recorded. Also, a proof version of the transcript following the hearing will be provided to you. All transcripts will be made public and posted on the committee's website. Welcome. Can I introduce from Allens Hub for Technology, Law and Innovation Professor Lyria Bennett Moses, also Siddharth Narrain, PhD candidate and Scientia scholar at UNSW Law. You will be provided with up to 10 minutes of a brief to be then followed by questions from the committee. Thank you.

Prof. BENNETT MOSES: First of all, thank you very much for having us here today and the opportunity to give evidence, for which we are very grateful. I would also like to acknowledge the Indigenous people of the land on which I meet here in Sydney and pay my respects to their elders past, present and emerging. My name is Lyria Bennett Moses. We have Siddharth here as well. The third author of the submission could not make it to this hearing, so if there are any matters on which she would be the best person to respond, we might have to take those on notice. But without anything further, over to Siddharth.

Mr NARRAIN: Thank you to the committee for this opportunity to be part of the proceedings. My own expertise is in Indian law around online hate speech, but for the purposes of this proceeding I will focus on two points which I think apply across jurisdictions. Reading all the submissions online that have been made so far has really helped me understand the Victorian context better and appreciate really how important the task of this committee is.

The first point is the role of anti-vilification laws in general, and a number of the submissions to the committee have focused on how ideally an anti-vilification law should both address incitement of third parties as well as the direct harm that is caused by vilification. In this category I think we have highlighted in our submission two effects of vilification. One is on the dignity of individuals, which really impacts the way that they can function and their civic status, and the second is what scholars call the quality of assurance that people have in society, which is that it actually threatens their sense of physical security and safety and thereby impacts the way that they can also function normally.

Any laws that are passed to regulate vilification have two functions. The first is more obvious—that is, of course, the fact that it is a deterrent value to people who potentially would indulge in hate speech. But the second, which we focus on, is what we call the more symbolic value of such vilification laws. I think this is what we call the expressive role of the law—that is, that by the very virtue of actually going through this process and enacting these amendments, broadening the protected characteristics and streamlining the provisions to address contemporary concerns such as online hate speech the Parliament of Victoria will be sending out a very strong signal in support of vulnerable communities and will be setting a standard of what is acceptable and what is not in Victorian society. I think this has been borne out by studies conducted in New South Wales on the civil laws related to hate speech by professors Luke McNamara and Katharine Gelber. I think this function speaks to the concerns of both security and dignity.

The second point I would like to focus on is really the role of online hate speech. I notice that a number of submissions so far say that online hate speech is just another version of hate speech and should be looked at that way, but I think online hate speech has certain specifics which make it particularly challenging to address. Two of these characteristics are the sheer volume of vilification that you deal with, and secondly, what we call acceleration of virality—the fact that almost instantaneously such content can be shared and goes through different mediums. Online hate speech coexists with more traditional forms, so it is not as if it operates alone. We saw this case in Myanmar recently, when there was a lot of attention around the content vilifying the

Rohingya community on Facebook but very little attention was paid to what the state-owned newspapers were doing, and both of these were functioning together.

The other point is that online hate speech also moves very easily between platforms. So something that I post on Facebook can end up on Instagram and can easily make its way onto WhatsApp and circulate. So all these things make it particularly challenging to trace and prosecute online vilification. I will hand over to Lyria to talk about some of the issues related to enforcement.

Prof. BENNETT MOSES: Thank you very much. I guess what I want to focus on is the challenge with online hate speech, particularly on social media platforms or on particular kinds of web pages and so forth, and how law enforcement goes about monitoring that, detecting vilifying speech, and obviously onto the question of actual enforcement.

Sometimes, obviously, law enforcement are notified of an occurrence—someone reports it—and that can generally be dealt with in the usual course. That is not really so much where the challenge lies. But also a lot of law enforcement agencies around Australia—and our research was quite general; it was not specifically or exclusively focused on Victoria—are also wanting to use automated tools to detect certain kinds of speech that they are particularly concerned about. That can be around particular events, that can be around particular hashtags that are being used at particular times on Twitter and so forth or it can be around known offenders—so people who are known by law enforcement as engaging in this kind of speech and they want to monitor what they are saying now. The challenge is that the current law does not really provide a very clear legal basis for that kind of automated analysis, whether it is of social media feeds or of websites or anything else that law enforcement wants to set up, and that can be potentially problematic.

Some examples of the kinds of problems we picked up. The first one is actually just a contract problem. So if you want to monitor what is happening or get particular kinds of feeds from Twitter or Facebook or anything else, you have often got to use a back end into their platform; just doing a Google search is not going to give you the kind of feed you need to automate your analysis. Now to do that, you ultimately have to sign up to a contract to be able to do that kind of analysis. The challenge is that the contracts being imposed by many of the social media providers put restrictions on. Some of those restrictions are framed in terms of, 'You can't use this platform to do surveillance'. Other ones—and different platforms do different things—can be framed around not being able to use personas, for example, which is what law enforcement often wants to do when it goes on these platforms so the individual police officers do not use their own names when they are monitoring. So there are those kinds of challenges.

The second set is around how privacy law interfaces with this. Obviously privacy law, in every jurisdiction including Victoria, is not just about secret information; it is about personal information. So even if something is public on Twitter, completely open to the world, the privacy laws still apply around how that information might be collected by law enforcement. With most of these automated tools you are not just reading stuff, you are actually collecting, because that is how the automated tools work. What that means is not that law enforcement cannot do it, because there are lots of rules about the circumstances—there is not a prohibition on the collection of information—but it does mean that there is a need to look at, for example, privacy policies and ensure that the transparency requirements in that legislation are complied with. If you actually look at privacy policies of law enforcement agencies even around Australia, not many of them are very clear about whether they are doing this kind of thing, how they are collecting the data, do they delete afterwards and so forth, which is the kind of transparency you would expect around this sort of thing.

The third issue we raised has moved on from when we raised it in the submission, which is access for evidence and particularly the difficulty of getting, and the time it takes to get, authenticated information from companies in the US such as Facebook to demonstrate that someone did say something, which if you want to ultimately prosecute and so forth you need to do. There is actually movement now at the commonwealth level on that and a move towards an agreement between Australia and the US, so that has moved on a little bit. But that is now really a question that the Commonwealth is dealing with.

The final point is to say that what I suppose we are arguing for here is a clear legal framework that enables the kind of surveillance that as a society we would consider reasonable in this context but does so with clear limits

and oversight, where those limits are not set by platforms but are set by Parliament. In other words, it should not be Twitter that decides whether law enforcement can do surveillance; it should ultimately be governments, and it should also be transparent. So if government law enforcement agencies are going to do this, then that should not be something that is hidden. That should be open and public and part of the legal framework under which that kind of surveillance can take place, including any limits on that.

We also made a point just at the end there about working through this. It is not only police that might want to do this kind of surveillance but also NGOs, academia and so forth to better understand the challenges of hate speech. Thank you.

The CHAIR: Thank you very much for your presentation. I will open up for questions from committee members.

Mr NEWBURY: Thank you both so much. It is a really fascinating area that you spoke on today. Can I ask you to set aside jurisdiction and law—and I know that is a really big set aside for a moment—and can I ask your view on de-anonymising? What is your view? It concerns me that if you publish something in certain forms, you have both civil and potentially criminal rights if you are the victim of that, but if you do it on Twitter or in certain social media forms, you have no capacity to know who the person is, and the criminal, for want of a better term, has a total right to do that. I would be really interested, generally speaking, what your views are as to whether or not you agree that there could be an issue with that and any insights you might have even internationally as to how you could address that.

Prof. BENNETT MOSES: Just to clarify the question: you are talking about the anonymity of the offender, so the fact that they are putting a post on social media under a pseudonym?

Mr NEWBURY: Yes.

Prof. BENNETT MOSES: Siddharth, I do not know if you wanted to say anything. My short response on that is I am not sure you can change the whole internet so that people can only speak on the internet—whether it is through social media platforms or their own websites—with full disclosure as to their identity. That would be a very significant change. I am not sure that is practicable, and I am not sure anything that would happen in Victoria would be able to make it so, even if it was a good thing to do. This is really tying in, though, with what I was saying about the platforms and in terms of getting information from the platforms. Even if I post under some kind of pseudonym, typically others will be able to identify me through my IP address and then going through the IP provider. There will be mechanisms at the back end, even if the victim cannot see who I am, that mean that if you get all the relevant companies to cooperate — unless I go above and beyond and start using Tor networks and so forth—most of the time I will be identifiable.

The real challenge is the time limits of that, and that is really where the commonwealth legislation, as I understand it, will come in to make it easier for Australian law enforcement agencies to be able to access that kind of information where it is stored overseas. Obviously where it is internally within Australia, which is relatively rare in a lot of these contexts, there are obviously existing law enforcement powers to do a lot of that stuff. But the delay at the moment, as we found in our research, was getting information from foreign companies. Does that answer your question?

Mr NEWBURY: It does, and I think it also points to one issue that, if you went down that path, might need an answer.

Prof. BENNETT MOSES: Sorry, I am not sure what—

Mr NEWBURY: I just was making the point that on the time limits issue, if you were looking at that, you would need to address the time limits issue.

Prof. BENNETT MOSES: Absolutely, and that is what the legislation is going to do. I should say we also did a submission to the commonwealth on that Bill, and there are certainly many ways in which the Bill can be improved on a number of dimensions, including legal protections, but rather than go into those here that is probably—at the moment, at least, I think—largely in the Commonwealth jurisdiction. Sorry I mentioned jurisdiction; you told me not to. Siddharth, did you have anything on that point?

Mr NARRAIN: Just to add a very small point that internationally there has also been a debate on the fact that anonymity is also kind of central to many of these communities that are targeted by hate speech—for instance, LGBT communities and so on. Online anonymity is often a way that they inhabit the space, so when you break that there are also consequences that one has to consider.

Ms SETTLE: Hello, and thank you for presenting. It is really interesting to hear. A lot of what you were talking about was around the police ability for surveillance. From another perspective, one of the previous submitters today talked about New Zealand law and New Zealand legislation, which was more around enabling people to report. What do you think of the New Zealand law that they were talking about? Do you think we need to have ways for the individual to report and to be followed up, or do you really see the solution as coming from the surveillance end?

Prof. BENNETT MOSES: I should say I do not actually have a view on the extent to which the solution should be from the surveillance end or not. My point there was largely: if that is happening, we should have a proper legal framework around that happening rather than a bit of an ad hoc situation we have now where what is happening could very well be breaching contracts or so forth. So it was not necessarily advocating for that mechanism. I am not familiar with the New Zealand legislation, so I will not comment on that. Obviously I think it is useful to have a mechanism where people can report—and report in ways that go not necessarily just to the platforms. I think at the moment there is lot of reporting through the platforms, a lot of concern about how that works and whether the platforms pick it up and whether the platforms are biased. I think you can work with the platforms, but I am not sure this is just a question for the platforms to make a decision about what is okay and what is not. I think there are definitely roles for other organisations there.

My only concern would be that if there is a reporting mechanism set up, that does not go to, if you like, a well of nowhere. We have had reporting for a while, for example, around scams, cyber-scamming and all those kinds of things. I have reported to that, and I do not know if anyone else has here, but it feels like it goes into a void. You do a report, they thank you for your report and there is nothing after that. I think if there is going to be a mechanism, you would only want to do that if you could assure the public that it would be taken seriously, that the reports would be read and acted on or, at the very least, if they are not going to be acted on—if it is a spurious report, for example—that they would be followed up.

Mr SOUTHWICK: I just wanted to follow-up on that in terms of accountability, particularly over big multinational international brands. Have there been other jurisdictional ways of being able to, say, make Facebook more accountable and social media more accountable for some of their stuff? What are some of the levers that we could be looking at doing, do you think?

Prof. BENNETT MOSES: Siddharth, did you have anything on that?

Mr NARRAIN: The most proactive on this front have been countries like Germany. Germany has enacted something called the *Network Enforcement Act*, which makes it compulsory for platforms to maintain records of such instances. So if somebody is breaking the law, not only do they have to report, they have to take action within 24 hours, and they have to be proactive in putting out statistics. If they do not take action, there are very, very heavy penalties that are imposed on these platforms. Of course there has been a debate around whether this has led to a kind of chilling effect and so on; there is an ongoing debate. It is a three-year experiment that they are conducting to see how the law works.

Prof. BENNETT MOSES: I would agree with that. I think it is a really challenging question as to what extent one wants to delegate to the platforms. The platforms will have their own agendas that do not necessarily align with what the Victorian Parliament is trying to achieve through legislation like this. Realistically when platforms are doing the monitoring it is being farmed out to click workers, often very low paid and probably not from within the jurisdiction or understanding any of the Victorian context, who are then making decisions about what is in and what is out. I am not saying there cannot be trial mechanisms for having that partnership work better, but I do think it is a very challenging space.

The CHAIR: I think that concludes the hearing. Thank you so much for presenting here today. The next steps will be that the committee has numerous other public hearings and submissions to deliberate on, and once those have concluded the committee will hand a report with some strong recommendations to government on

this important matter. But again, on behalf of the committee, to Lyria and also Siddharth, thank you so much for being here and taking the time to present to us.

Prof. BENNETT MOSES: Thank you very much for the opportunity.

Mr NARRAIN: Thank you so much.

Witnesses withdrew.