ELECTORAL MATTERS COMMITTEE

Inquiry into the Impact of Social Media on Elections and Electoral Administration

Melbourne—Monday, 1 March 2021

(via videoconference)

MEMBERS

Mr Lee Tarlamis—Chair
Mrs Bev McArthur—Deputy Chair
Mr Enver Erdogan
Mr Matthew Guy
Ms Katie Hall
Ms Wendy Lovell
Mr Andy Meddick
Mr Cesar Melhem
Mr Tim Quilty
Dr Tim Read

WITNESS

Mr Tom Sear, Industry Fellow and PhD Candidate, UNSW Canberra Cyber, Australian Defence Force Academy.

The CHAIR: I declare open the public hearings for the Electoral Matters Committee's Inquiry into the Impact of Social Media on Elections and Electoral Administration. I would like to begin this hearing by respectfully acknowledging the Aboriginal peoples, the traditional custodians of the various lands each of us is gathered on today, and pay my respects to their ancestors, elders and families. I particularly welcome any elders or community members who are here today to impart their knowledge of this issue to the Committee or who are watching the broadcast of these proceedings.

I welcome Tom Sear, Industry Fellow and PhD Candidate, University of New South Wales Canberra Cyber, Australian Defence Force Academy. I am Lee Tarlamis, Chair of the committee and a Member for South Eastern Metropolitan Region. The other members of the committee here today are: Bev McArthur, Deputy Chair and a Member for Western Victoria; the Honourable Wendy Lovell, a Member for Northern Victoria; Katie Hall, Member for Footscray; Andy Meddick, a Member for Western Victoria; Cesar Melhem, a Member for Western Metropolitan; and Dr Tim Read, Member for Brunswick.

All evidence taken by this committee is protected by parliamentary privilege. Therefore you are protected against any action in Australia for what you say here today. However, if you repeat the same things outside this hearing, including on social media, those comments may not be protected by this privilege.

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, PowerPoint presentations and handouts will be placed on the committee's website as soon as possible.

I now invite you to commence with an opening statement introducing yourself and what you consider to be the key issues. To ensure enough time for discussion, please limit your opening statement to about 5 minutes.

Mr SEAR: Thanks for that, and g'day everyone. I guess most broadly I want to emphasise how social media has altered politics and the function of politics itself. Deception is kind of a feature both in nature itself and sort of in upper hominids like us, so in social media equally it is part of human society, so deception is kind of a feature and unfortunately not a bug of the systems and the way in which humans operate with them.

What has happened with social media and politics is that we have moved to sort of a very data-centric mode of politics, which kind of reflects the turbulence of natural systems in a sense. It is about fluid dynamics, it is very turbulent, it is about entropy and exponential climbs, which means that things go viral very quickly. And that means we have moved into a politics of time really and it is less about who says what but maybe when they say it and what works in terms of that. It is also a function of media ecology, so we will see mainstream media function with social media amplifying and de-amplifying material, and I guess the classic case is hashtag politics like 'I stand with Dan' and 'Dictator Dan' in Victoria, language you can get a hashtag trending, you use sock puppets to oppose them, then the mainstream media will say, 'Oh, this is the popular view', and so on and so forth. And that is partly because the social media we have is based around a mid-century social science or sociometrics model which is based around activism and individualism. And we have seen opposing sites on Wikipedia just this morning, for example, around some federal issues.

This means that we have got the problem of asymmetric data management. So if you own the vector, you can manage politics, and the people who own the vectors now are the people that own the media companies, and that is obviously the [inaudible] all the way into states like the media in the People's Republic of China, for example. So if you control those vectors, you can manage and manipulate politics across borders. So as well as states thinking about their cybercraft, Victoria is going to have to think about what is digital Victoria, what is a silicon state now—I mean, we have seen through COVID a lot of interrogation and an increasing focus on borders. What is the silicon state? What is the Victorian state-centric position in cyberspace, and what is the data of Victorian citizens and what does it mean?

In terms of foreign intervention, for example, I recently just published a piece which is about, as you might know, the Russian Internet Research Agency and its influence on the US election. Through the same period it also targeted Australians in a minor way, and one of the ways it actually did that was something we have just been through, which is the Australian Open. So the Internet Research Agency used a lot of hashtags and a lot of

material to target Australians around sport. And the Australian Open, because of Sharapova's particular drug testing, was a focus for that organisation, so it brings in issues like culture. You will not always influence politics in the way in which you might expect. You will not say, 'Oh, this is a bad thing about an election' or, 'So-and-so said this'. It is about how you might move polarities and restructure and reframe discussions.

To that, I suppose a lot of my work with my colleagues has been around the role of Chinese-based media in Australia and the way in which PRC-centric media is influenced by what we might call the overseas Chinese affairs office—which we might call the magic weapons of the overseas affairs office in the PRC—and the way in which certain media companies in Australia have ownership associated and goals associated with PRC-based entities to influence, for example, the Chinese diaspora in Victoria, and we could discuss the various accounts which might function that way specifically. Certainly, as ASIO has indicated, we are seeing an unprecedented influence from the PRC in Australia, and some very close data analysis of, say, WeChat in Australia indicates that media is being influenced. And you can influence media I guess, looping back to my opening point, in elections at times where we have got an election that is very, very split and often is divided and it does not take much to win government, if you can influence a small population in a small area, then you can win a seat and so on and so you get this rolling effect where if you influence opinion, you may be able to influence an election.

So I guess I am emphasising that Victoria might think as a big picture about what these asymmetric data relations are about for citizens. You can talk about regulation if you wish of course, but what it means strategically for the future about how to manage future elections and how electoral politics function with the various communities and how communities can really in a digital environment respond, because they are very much an analog entity, and so on and so forth. I think that is my 5 minutes. Thank you.

The CHAIR: Thank you. Now, in terms of opening up for questions, Dr Read, did you want to kick things off?

Dr READ: Yes. I am curious to know to what extent influencing the diaspora of any country—obviously China comes to mind—is important in influencing election outcomes. My question is: when people become citizens and obtain the right to vote they have usually been here for a while. Do they still retain links to their home country sufficient to participate in things like social media and be influenced by it? Obviously they do not shed all their cultural links and so on, but do you think that it is still significant? Do you think that is a lever?

Mr SEAR: Yes. Certainly the Chinese Communist Party believes that it is, and they act in that way in order to influence those populations. And of course caveats, generalisations about cultural populations obviously occur in this situation, so we have to be careful the way in which we frame these things of course. But if we were to generalise: say we would estimate the diaspora of ethnic Chinese people in Australia—citizens or otherwise—at 1.2 million, 1.3 million people. I would expect at least half of that community are actively engaging with the accounts we are discussing. They would be engaging in private discussions in those places, but also nearly all of them that are involved are following what we call 'official accounts', for example. Official accounts, we know, are influenced by the Chinese Communist Party and they frame debate a bit—as we were discussing about the Russian example—in certain specific ways to influence those environments. I mean, again this is a generalisation. I am obviously a white, Anglo-Celtic male and my family come from Scotland and Ireland seven, eight generations ago, but obviously I still have an engagement in those places and those communities even that far back. So, just speaking for myself, I am influenced by some of those cultural views. The way you tend to produce cyber-influence now, in a formal either military or governmental sense, is through cultural ties. So if cultural ties remain, then there is an opportunity, yes, to influence them.

The CHAIR: Thanks. Ms Lovell.

Ms LOVELL: No, I do not have any questions, Lee, thank you.

The CHAIR: Mr Meddick.

Mr MEDDICK: Thank you, Chair, and thank you, Tom. It is a fairly extensive submission you have put in there. I confess I did not get as much time as I wanted to to have a look at the section around geopolitical information in the Indo Pacific, for instance. I have got a number of questions, but first of all I wanted to refer to you talk about that it is best to defend a political society from each country's unique cultural standpoint and that we need a uniquely Victorian response. What does that actually look like? Can you give us some sort of an idea of what a uniquely Victorian response looks like? Then with that in context, a lot of what you are talking

about here does refer to your experiences and your research around the CCCP, but have you gone any way down the rabbit hole of the far right as well? Because we keep hearing about the greater influence of the far right around the world and here in Australia. We have seen it in terms of public demonstration, and they are getting bolder. And they are also using social media in a very canny way. Have you gone down that path at all, and are there any warnings or any advice that you can give us now about how to try and curb that activity?

Mr SEAR: In a military sense we talk about strategic societies, and probably the best example really is Victoria's response to COVID in the midst of the crisis. I caveat again: I grew up in Sydney, so there may be some competitive city things going on here. But that is indicative also of how you develop a culture that is consistently around place, for example, or is around cohesive responses to certain scenarios. Melbourne's very cohesive and Victoria's very cohesive response to the crisis in COVID is a very precise example of the type of activity we are going to see politically in the 21st century and how you build communities around that and how you do not.

I guess speaking of course to the influence of right-wing groups, we also saw there the way in which, say, influencer culture in Melbourne was very critical in swaying opinion toward public displays of demonstration, which, as you suggest, borrow very much from international forms of right-wing activity, and then do deploy those in influencer and Instagram environments, for example, to quickly scale up very rapidly. So in a sense they are similar in the way in which geopolitical trends occur.

For example, we might see something like 5G. Say we saw 5G developing sort of out of the United States and perhaps in parts of Europe in March. You will see it in Instagram culture fairly quickly, but then perhaps there will be some peak accounts which, during the midst of the lockdown in Victoria, will suddenly escalated their activity and became very prominent. It is not dissimilar in terms of how you would track the way in which those influencers happen. It is slightly easier in that state-sponsored activity is usually associated with large-scale media control, so the far right tends to operate as much more a loose coalition in social media and is kind of dependent upon individuals under the sociometrics we were talking about earlier. So it is a bit harder for whack-a-mole, and of course the unfortunate case with the terrorist activity in New Zealand is an example of how you would suddenly be tracking that. Obviously that is on many people's radar in the intelligence community, I can tell you that. There is concern around those spaces about how to best examine and explore those critical issues breaking out.

Mr MEDDICK: And I guess as well it becomes then a fine line of balance between what you determine as something that should be shut down or at least inhibited versus broadscale censorship.

Mr SEAR: Right. Then you have got the issue of what is speech. How does speech function in Australian society? How does speech function on a platform? You will notice that platforms are very conscious at the moment to be thinking about framing speech in relation to their procedures and their policies. It is partly because big tech is interested in you guys kind of regulating, because as bigger organisations they can pivot in regulation very, very quickly. Perhaps what is more concerning when you examine the way in which big tech might have responded to electoral issues in Australia is the speed with which they—when you examine FOIs, for example, the slowness with which these big tech companies have previously responded to your queries and questions of, say, the AEC or the Victorian Electoral Commission in an era where time is critical. So 'take down' and 'speech' are also different. Take down could be managed algorithmically. For example, in terms of take down in Australia, we are kind of a cybercolony in a sense, or an information colony, perhaps to some extent the United States and China to some extent too. What they will use is AI that is distributed, and the challenge really is how that AI works across the planet more. So shut down is not so technically difficult as speech management, as we have seen of course in the United States in the last year.

Mr MEDDICK: And do you have any figure in mind at a Victorian state level then—a dollar figure—for what it would cost the Victorian taxpayer to develop an algorithmic response to a militarised, if you like, political campaign that is done through social media?

Mr SEAR: That is an interesting question. Certainly it would be quite cheap for you to create dashboards which monitor those environments. They are not very expensive to create at all. You could almost create ones which do live monitoring of activity and estimate certain misinformation or disinformation activity that is going on. For example, my colleagues and I were tracking Chinese and Russian propaganda in the Australian federal election. I think we just did a live capture in those two months, six weeks preceding the 2019 election. It is not difficult to capture live probably about maybe 4.8 million tweets and then maybe a million other datapoints

across other social media, and you can do that almost with a decent PC with a few cores in it and the appropriate piping scripting. So that is not difficult. But then of course you get into the question of if speech is happening on a platform, do you then begin to control that speech in an algorithm response, and what would you do? How would you frame it? Obviously in the Russian case it was not about necessarily disinformation in the sense of, 'Here's a fact'. You will find that fake news is kind of fake news, to be honest with you. Most propaganda is an extension of a fact or a distortion of one particular fact and reframing it rather than about something being wrong or fake news. That makes it so hard to control speech or manage speech in a particular environment, because what are you doing? It would not be difficult or expensive to run some scripts which might identify it, but then you have got the question: when does censorship kick in? And we go on from there.

Mr MEDDICK: Great. Thanks, Tom. Thanks very much. Thanks, Chair.

The CHAIR: Ms Hall.

Ms HALL: Thank you, and thanks for your very detailed submission. I am interested in microtargeting. I do not know much about it or how it works, but I am interested in your I guess perspective on how it has impacted elections in an Australian context and how it could continue to influence elections at all levels of government.

Mr SEAR: Good question, because what are the internet and these big platforms for? They are about telling us things. And how do you do that? You do microtargeting. I point you to the most recent report by the ACCC, which is a 222-page report which examines in detail how advertising and microtargeting actually function. I guess in the last 18 months yes we have seen microtargeting based on advertising increasing emphasis in Australia. Obviously in a federal election the most famous case is a very warped individual that sent small text messages saying, 'We shouldn't get all these text messages all the time'. The irony is deficient, but the capacity to demonstrate that reach is really what that message was about and saying, 'We know who you are, we know where you live and we know everything about your particular patterns'. And of course the famous Facebook example, which was Cambridge Analytica, is literally the big five, which is what those in academia had used before, which is the way in which you identify humans in a [inaudible] personality in social media. And then you go and target them individually, whether that was effective or not.

But I think we are seeing an increase. Certainly in the US election, that is where the money went on advertising in the last election—it went into microtargeting. Microtargeting—the debate is open about whether bubbles exist, but probably mathematically social media tends towards bubbles, which means you can target someone and begin to influence them and then, in the ecology of the information environment, even construct even more information around them, which will influence them even further. In the military you always attack a strategy. You do not attack what someone is doing, and the strategy in social media is around advertising data. So the challenging bit is if you wanted to do something to the Victorian settings you probably would look at the asymmetric nature of their data relationships with these big companies and go after that in regulation and procedure.

Ms HALL: Thanks very much.

The CHAIR: Tom, in terms of microtargeting and things like that, Facebook have their ad archive, which does not capture all ads, including a lot of the microtargeting. Some of the submissions that we have heard have been around the need for a proper ad archive that would capture political advertising, which would be potentially real time and would include all information around all advertising, including who they are targeting by age demographic, how much has been spent, how many clicks it has got, who had paid for it—all of that sort of stuff—and that is easily searchable and accessible to anybody. It would provide a lot of knowledge about who was doing what and would also be able to sort of counter that narrative where if there was a scare campaign being run or a negative campaign that was misleading, it could be countered. Is that something that you think would be helpful?

Mr SEAR: Yes, the global academic community has a sort of paradoxical relationship with the Facebook ad archive. On the one hand, yes, we see it as a productive force to be able to understand precisely what is going on, and it is obviously a positive outcome. As you describe it, yes, that would inform citizens much more about what is happening. One of the questions is: how quickly can it really respond and how comprehensive is it? My colleagues at the Oxford Internet Institute have done some close analysis of that ad archive in the European elections in particular, and they had some concerns about whether it really reflected reality and how things

could be influenced. So I would point you probably to those studies to look at—whether it was really representative of what was going on.

But also, is advertising how you would run a disinformation campaign? Yes, you might target ads through something like that, but influence and how material spreads is equally as important as how someone is specifically targeted by a campaign and whether it exists or not. Certainly, yes, we need more live capture and transparency around the way in which political advertising takes place and who is paying for it and where the sheer volumes of it are and how you are being targeted. It is somewhat of a black box for us all as citizens as to how we are targeted, so even explaining that to people would be of great benefit, but really the question is: is the ad archive enough, and is the oversight board's understanding of the ad archive really sufficient? Some consensus in the global academic community is no, that it is not sufficient and there needs to be far more active measures around the way in which the transparency of our data is being managed by these companies to be used in these campaigns.

The CHAIR: Yes, I think that is right. I think it might be one of the tools in the toolkit, if you like, not the entire solution, and again, it is probably more targeted to domestic politics as opposed to capturing the international players who are more likely to operate through bots and sock puppetry and all those sorts of things. The other question then is: if you were to look at doing that as one of those tools, would you have any views about—the big question would be—who would actually be best placed to operate such an archive or be the keeper of such an archive? It is another live question. Do you have a view on that?

Mr SEAR: Yes, it is a difficult problem, and it really is partly because our democracy—our governance, our society—is kind of stovepiped or siloed in older forms of media, older forms of democracy, and we have suddenly all been swamped by a swathe of social media. At the federal level I would advise the federal government to run task forces. You have to really spread the expertise across the government, and so in that case I would advise the government to run task forces across home affairs, defence, ASIO—all of those entities—the AEC. We learned in a campaign against ISIS which was called Glowing Symphony, whereby you would quickly get task forces up—because the problem is, as you know as politicians, in government people have their fiefdoms and their authorities of control and their decision-making powers and they like to stay within them or maintain them, and these measures are designed to spread across those and disrupt those particular silos. So you would have to develop task forces, and ideally you would have a task force which had even those from civil society and members of the public who may be a bit on the model of democratic citizenry-type parliamentary options with those people who understand human rights et cetera. So you can get a balance to what is actually happening and get the public's view and also the public's understanding of how they experience politics, how they experience this information. So it is a bit of a broad-ranging strategy across who would be doing it, because obviously you have got the problem in any democracy: if you give too much power to one group, then they will also seek to influence it, whoever they are, so you want to be trying to distribute that. But obviously you would have to be involving the company, so all the major platforms would have to be actively involved and transparently involved in how that would take place, and that includes all the international companies. And then we have the challenges of state laws, federal laws, media laws, media ownership laws. Your capacity to leverage those people to be involved is also a challenge as well.

The CHAIR: Yes. Okay, thanks. Are there any other questions from committee members? Yes, Dr Read?

Dr READ: Thanks. If we have got time, Chair, I wonder if we could ask Tom to talk a bit more about the recommendations involving the Victorian government cybersecurity unit and the chief information security officer. I notice you have made a number of recommendations around making more use of them.

Mr SEAR: Right, exactly. We do not discriminate in military or information operations between cyber and necessarily information operations anymore. But, for example, in the famous cases you know about, like the hack and leak in the United States, that was probably more effective than any, even the IRA activity, in influencing, and even perhaps in the media activity. So if you really wanted to do an influence operation, you would be involved in some sort of cyber intrusion to extract data from someone, a power or an entity, and use that information against them. So that means that as much as we might defend the strategic society in social media, which is really kind of our critical infrastructure now, we need to think about other critical infrastructure—so the way in which political parties defend themselves in terms of a cyber sense, the way in which the Victorian Parliament is able to defend itself in terms of what we might call hard cyber, like networks, email, databases and so on and so forth. In order to really defend yourself in the information space, you have to be involving those people who know, and it is those people that you are describing that really understand how

you would defend the Victorian government from a whole series of nefarious attacks and defend yourselves, politicians, from being breached and an active measure against you or an active measure against a particular society. But even if someone was to go on very quickly, those guys and those women will know best how to develop code very quickly to respond to and defend against those particular networks. So you could even just sit down and say, 'How do we do this?'. If we are moving into IoT, for example, there are codes of conduct around the Internet of Things, even at that level, those cyber entities as opposed to even media—I guess we are moving away from statecraft and into cybercraft. And a lot of governments defend critical infrastructure like water, power and everything that is keeping the lights on here, but really now social media is a form of critical infrastructure for Australian society, and unless we begin to involve our cyber experts in that space—state level, federal level—we are going to be in trouble in the 21st century.

Dr READ: Thank you.

The CHAIR: Are there any other questions? No. All right. On that basis, can I thank you for your submission and also coming along and talking to us today. It has been very insightful and helpful with our inquiry. There may be some follow-up questions from committee members following today. It would be great if we could pass those on through the secretariat. Thank you again for your time today. It has been great.

Mr SEAR: Yes, it has been good—good questions. Thank you.

The CHAIR: Thank you. And that ends today's session. Thank you.

Committee adjourned.