EMC Submission No. 98
Received 30 September 2020

CENTRE FOR DIGITAL RIGHTS

September 30, 2020

BY EMAIL ONLY

emc@parliament.vic.gov.au and lee.tarlamis@parliament.vic.gov.au

Mr. Lee Tarlamis, OAM MP
Chair, Electoral Matters Committee
Parliament of Victoria
Parliament House, Spring Street
East Melbourne VIC 3002
Australia

Dear Mr. Tarlamis,

Re: Parliament of Victoria's Electoral Matters Committee (**EMC**)'s inquiry into the impacts of social media on elections and electoral administration (**EMC Inquiry**)

Thank you for the opportunity to make this submission to the EMC Inquiry. Your August 11th letter of invitation is addressed to me as Chair of the Centre for International Governance and Innovation (**CIGI**) a well-known, global, non-partisan think-tank that I founded in 2001. I am pleased to respond to your letter in my capacity as President of the Centre for Digital Rights (**CDR**) a newer, non-partisan not-for-profit organization that I founded in 2018 in the wake of the Facebook-Cambridge Analytica scandal.

THE CENTRE FOR DIGITAL RIGHTS AND ITS RELEVANT EXPERTISE

CDR aims to promote public awareness of digital issues related to the data-driven economy in three ways – namely, by:

a. advancing the public's understanding of their rights;

b. raising policymakers' understanding of advanced technology; and

c. promoting best practices, laws and regulations that protect both the civic values and the rights of individuals in the 21st century economy, driven by the mass collection, use and disclosure of data.

Since May 2018, CDR and others in Canada (including civil society groups, journalists and academics) have been raising urgent concerns about the data protection practices and policies of

Canada's federal political parties. CDR has held discussions with several Canadian law enforcement authorities that administer principles-based legislation on competition, privacy, anti-spam, malware, and election integrity.

CDR has also submitted or supported complaints to those authorities. The complaints focus on the problematic privacy practices of Canada's federal political parties, especially in the context of their development of voter relationship management (**VRM**) systems. These systems collect personal information on Canadian voters (often without their knowledge and consent), develop highly personalized profiles on each voter, and then score these voters usually on a sliding scale (e.g., as someone who supports the party, someone who doesn't support the party, or as someone who is undecided and so persuadable). The VRM systems are then deployed to deliver selective, micro-targeted political advertising most often on social media platforms (and most notably on Facebook). The pernicious nature and manipulative effect of these VRM systems on democracy has been researched and documented by many experts, including Professors Jacquelyn Burkell and Priscilla Regan in "Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy," (December 31, 2019) 8:4 Internet Policy Review where they conclude:

> *When political communicators have the advantage of deep and detailed knowledge about the public and when they leverage that information to develop and deliver political messages designed to persuade specific individuals based on what is known about their demographics, personality, attitudes, beliefs, etc., and when those messages take advantage of persuasive principles drawn from the empirical literature in order to exploit a predictable interaction between individual and message, the result is an unfair system that undermines voter autonomy*.

That such sophisticated data-driven VRM systems can and have been weaponized and deployed for fundamentally undemocratic ends is often in the news. See, for instance, this September 28th story from Channel 4 news in the UK: Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016

Also on September 28th, CDR submitted a 30-page response (**CDR's Response)** to Elections Canada's consultation on Political Communications in Canadian Federal Elections in the Digital Age (**EC Consultation**). A copy of CDR's Reponse is attached to the cover email for this letter. Given the common focus on social media and political communications in the EMC Inquiry and in the EC Consultation (especially its Discussion Paper 2: The Impact of Social Media Platforms in Elections), I urge that you review the well-researched discussion papers that grounded the EC Consultation and informed CDR's Response. Many of the issues discussed in these papers are global, not unique to Canada, and so they will be pertinent to the EMC Inquiry.

THE COMMON INTERESTS OF AUSTRALIA AND CANADA TO REGULATE US BIG TECH AND ESPECIALLY ITS IMPACTS ON DATA-DRIVEN ELECTIONS

I commend you on your work to date and note the constructive position that Australia's Federal Government along with Australia's federal competition and privacy authorities have recently taken on issues such as the regulation of big tech platforms for the public good. I am particularly encouraged that the Australian government is not bowing to threats by U.S. web giants that attempt to coerce you to play by their rules and thus seek to undermine your economy and sovereignty.

As you may know, Canada is facing many of the same challenges regulating big tech and mitigating the adverse effects of its toxic business model on Canada's economic, political and social well-being. For instance, just like Australia's enforcement authorities, Canada's competition and privacy enforcement authorities are currently engaged in protracted legal proceedings to stand up to big tech scofflaws like Facebook and Google.

CDR'S RESPONSE TO THE EMC INQUIRY'S QUESTIONS

In response to your questions, I offer the following observations and suggestions:

1. THE CURRENT (DATA-DRIVEN) BUSINESS MODEL OF SOCIAL MEDIA UNDERMINES PERSONAL AUTONOMY, INCLUDING ELECTORAL CHOICES

The online advertisement-driven business model subverts choice and represents a foundational threat to election integrity, markets and democracy itself. This is because technology gets its power through control of data. Data at the micro-personal level gives technology unprecedented power to influence. In my testimony to the International Grand Committee on Big Data, Democracy and Privacy, I said that data is not the new oil - it's the new plutonium. Amazingly powerful, dangerous when it spreads, difficult to clean up and with serious consequences when improperly used. Data deployed through the next generation 5G networks is transforming passive infrastructure into veritable nervous systems. It's also reshaping public square, civic discourse and elections everywhere.

Over the last few years, whistle-blowers from big tech companies have offered very valuable insights, including this quote: "*the dynamics of the attention economy are structurally set up to undermine the human will*". Democracy and markets only work when people can make free choices aligned with their interests, yet companies that monetize personal data such as Facebook (including its subsidiaries Instagram and WhatsApp), Google and others are incentivized by, and profit exclusively from, undermining personal autonomy.

It is crucial that lawmakers and regulators in both Australia and Canada (and indeed in any other country around the world that values a vibrant democracy and free market) know that social media's toxicity is not a bug - it is a feature. Technology works exactly as designed by those who create, and profit from it. Usage patterns drive product development decisions. Behavioural scientists were directly involved with today's platforms and helped design user experiences that capitalize on negative reactions because they produce far, far more engagement than positive reactions. This is why we are seeing historic levels of polarization even in countries with previously vibrant civic cultures and strong tradition of democratic institutions.

2. THE IMPACT OF SOCIAL MEDIA PLATFORMS IN ELECTIONS IS NEW AND REQUIRES UPDATED REGULATORY FRAMEWORKS

The realities of contemporary social media communications and data-driven elections requires a new framework to address transparency, fairness, and democratic rights. Key deficiencies contributing to the inability of any oversight regime to effectively regulate political communications through social media are the lack of technological capabilities addressing transparency, accountability and fairness, and the absence of robust, effective and enforceable privacy oversight respecting both communications and the communicators.

As noted above, for the past two years, CDR has pursued a Quinfecta of Legal Complaints against Canada's federal political parties to ensure that Canada's law enforcement authorities hold these political parties accountable under various Canadian laws regarding what these political parties do with Canadian voters' personal information – especially in the context of deploying their VRMs in data-driven elections. In preparing my submission to your inquiry, I was frankly surprised and disappointed to learn that Australia is an outlier in that it is one of the few western democracies (apart from the U.S.) where political parties are expressly exempt from privacy laws. Given CDR's recent experience dealing with how Canada's federal politicians collect, use and disclose Canadian voters' personal information without their knowledge and consent, Australia's privacy law exemption for political parties seems misguided (or at least ill-suited for today's world of data-driven elections). Consequently, I urge that the EMC give serious consideration to recommending that this exemption be eliminated.

Targeted communications require amassing diverse profile data about electors. The largely unregulated collection, use and disclosure of such personal information enables targeted political communications, in particular through social media. It is clear that the current regulatory oversight framework and technological capabilities cannot achieve full transparency, accountability and fairness in respect of political communications through social media. **In this context, targeted political communications through social media platforms are beyond the practical scope of any of the current regulatory regimes and as such have no place in the democratic electoral process. Consequently, they should be prohibited, at least until and unless an effective accountability regime and full privacy oversight is established.**

The Internet and social media present an entirely new playing field where diverse data tracking and targeting, now leveraged by political parties, is the norm. Therefore, political parties, candidates and their related organizations must be immediately brought within a strict and enforceable privacy oversight regime. It is important to note that under the EU's General Data Protection Regulation (**GDPR**), political opinions are considered "sensitive" forms of personal information, and (with limited exceptions) only collected with express individual consent.

Addressing the new paradigm by extending privacy laws would not only provide oversight of the political parties themselves, it would extend to the work that data strategists and influencers perform for the parties. Additionally, it would extend to advertising and other political communications carried on by powerful social media entities such as Facebook and Google. Under an enhanced privacy law, political parties would no longer be unaccountable for the actions taken on their behalf by such third-party actors. This new privacy paradigm should hold social media platforms and other big tech companies accountable for their data protection practices for political advertising through compulsory rules, as opposed to weak, voluntary policies.

Targeting potential voters through any medium involves collection and use (or "tracking") of personal information about them. A targeted social media message requires not only information about the individual's identity or characteristics, but also ancillary information such as socio-economic status, geo-location, likes and dislikes, and prior political inclinations. Having this information about an individual enables bad actors to craft persuasive messages exploiting misinformation that plays to their socio-economic, or even psychographic, profile. Regulating the conditions under which all this personal information legally may be collected by, or for the benefit of, political parties should be included in the expanded privacy protections.

3. POLITICAL COMMUNICATIONS IN THE AGE OF SOCIAL MEDIA NEED RELEVANT, EFFECTIVE AND TRANSPARENT RULES AND GOVERNANCE MECHANISMS

Just a few days ago, a whistleblower at Facebook said this about the use of their platform by political actors:

"I've found multiple blatant attempts by foreign national governments to abuse our platform on vast scales to mislead their own citizenry, and [that] caused international news on multiple occasions. I have personally made decisions that affected national presidents without oversight and taken action to enforce against so many prominent politicians globally that I've lost count."

Social media platforms remain the most powerful tools to manipulate citizens and have proven that they cannot be left alone to self-regulate let alone govern the public sphere for the common good.

"Election advertising activities" should be defined broadly to include all communications conducted by political parties and their third-party actors with a view to influencing the electoral decisions of citizens ("**political communications**"). It should encompass messages posted through social media and other digital communications, whether paid or unpaid. Additionally:

- all political communications should clearly and prominently identify the communicator and, if different, the person paying for the communication;

- all oversight of political communications should extend to both the election period and all periods outside of the election (given the modern reality of "permanent campaigns");

- recognizing the difficulties in policing false information provided through advertising activities and other political communications on social media, a prohibition should be imposed against targeted political advertising communicated through social media at least until an effective accountability regime and full privacy oversight is established;

- serious consideration should be given to the adoption of a rule prohibiting fundamentally inaccurate advertising in the electoral ecosystem as has been recommended in the June 29th UK House of Lords Report entitled Digital Technology and the Resurrection of Trust ;

- all political communications should be subject to record-keeping requirements. Records should be maintained in a central registry, maintained by the Victorian Electoral Commission (**VEC**) or a service provider, which could be a telecommunications company, accessible for public review. The ad registry should include sufficient information regarding the targeting criteria of the political party to enable an individual to know why they are seeing an ad; and

- the VEC should be given the power to ensure online social media platforms are transparent in how their algorithms work. This transparency should include reviews of training data (data the algorithm "learns" from), design bias and discriminatory outcomes in order to ensure that they are not operating in ways that discriminate or otherwise harm recipients of the platforms' communications (especially its political communications). To achieve this transparency, the VEC should publish a code of practice for political parties regarding algorithms.

To your question *"What are the most effective ways to address any problems with social media and online advertising around elections?"*, I offer following recommendations:

Our traditional democratic institutions, rules, and regulatory frameworks were not designed to deal with these emerging challenges but there is much your government can do to catch up. To preserve free and fair elections, including ability of private citizens to make decisions at the ballot booth free from behavioural manipulation, **we need to outlaw the current business model and re-introduce responsible monetization, such as subscription-based models**. Strategic regulations by government should ban hyper-personalized advertising by social media platforms or risk perpetually coping with the existing and emerging consequences which quickly turn policymaking into a losing game of regulatory whack-a-mole.

While disinformation, fake news and other forms of voter manipulation are increasingly and disturbingly undermining democracy, they are just part of the negative outcomes from unregulated attention-based business models and cannot be addressed independently of the broader need to establish rules of the road for data governance. **Governing data must be tackled horizontally, as part of an integrated whole**. To exclusively focus on specific challenges stemming from social media's role in various policy challenges such as the proliferation of online hate, conspiracy theories, politically motivated misinformation, harassment, and social media's impact on election is to miss the root and scale of the problem.

IBM recently estimated that 90% of all the world's data had been created in the previous three years. While profound in terms of its implications for the organization and governance of society and economy, the current shift is unprecedented in terms of its rapidity and thus demands sophisticated policy responses. I respectfully submit to you and your colleagues that the governance of data is the most important policy issue of our time because control of data is creating a new kind of social and political space in which both the public and private spheres are technologically re-shaped. **Data governance requires both national policy frameworks and international coordination.**

CONCLUDING REMARKS

I encourage you to keep up Australia's participation in the International Grand Committee because cyber space has no borders and the issues raised by social media and big tech platforms generally cannot be hermetically sealed at national borders. IGC meetings have included parliamentarians from Argentina, Australia, Belgium, Brazil, Canada, Costa Rica, Ecuador, Estonia, Finland, France, Germany, Ireland, Latvia, Mexico, Morocco, Singapore, St. Lucia, the United Kingdom and the United States. This is a powerful forum to create updated regulatory frameworks to fit the challenges of global social media platforms.

As your Committee begins its work evaluating the submissions put forward in this inquiry I urge you to resist a staggered approach to regulating social media and instead, respond swiftly and strongly to regulate its impact on Australian democracy. Technology is not governance; it must be governed. The choice citizens of democratic countries face is not between Facebook and China – which paradoxically borrow from each other the tools and tactics that encode their grip on power. The option we face is either a social choice mediated by democracy or social outcomes engineered by unbridled, unethical and unaccountable power.

I remain confident that Australian parliamentarians will preserve social choice and democracy. I look forward to reading your final report in June 2021 and, again, thank you for the opportunity to engage with your Committee.

[redacted]

Jim Balsillie
President, Centre for Digital Rights
Chair, Centre for International Governance Innovation