**MANAGING CANADIAN ELECTIONS INTO
THE FUTURE
*LE FUTUR DE L'ADMINISTRATION
ÉLECTORALE AU CANADA***

**Online Disinformation and Harmful Speech:
Dangers for Democratic Participation and
Possible Policy Responses**

Chris Tenove^{*}
Heidi J.S. Tworek^{**}

1. INTRODUCTION

As democratic countries prepare for elections, they must address a host of challenges posed by new digital technologies and the rapidly-evolving information system. Exchanges of views and information lie at the heart of electoral campaigns. But new developments in online communication may stymie the chances for candidates, political parties, civil society groups, and citizens to engage in free, fair, and informative public discussions. This is a complex policy area, which overlaps with issues ranging from cybersecurity to freedom of expression to the transforming media landscape to contemporary geopolitics.

The Canadian government has started to address these problems. In spring 2018, the government announced Bill C-76, the *Elections Modernization Act*. It includes new limits on third party spending, creates a pre-writ period, makes voting more accessible for people with disabilities, and requires social media platforms to create registries of political advertisements. On January 30, 2019, the Canadian government announced specific measures to safeguard the integrity and legitimacy of elections, including a federal task force to monitor

^{*} Post-Doctoral Fellow, Department of Political Science, University of British Columbia.

^{**} Assistant Professor, Department of History, University of British Columbia.

for potential interference and a protocol for civil servants to alert citizens about interference during an election campaign.¹ However, much can still be done to uphold the communications element of electoral integrity, both by government and by other stakeholders including journalists, social media companies, and civil society organizations.

This article focusses on two related challenges: disinformation and harmful speech online. By “disinformation,” we refer to intentionally false or deceptive communication to advance political ends. We use the term “harmful speech” to refer to communication that is abusive, threatening, denigrating, or that incites violence. We clarify the risks that disinformation and harmful speech pose to democratic engagement and democratic processes, and synthesize current research about their creation, circulation, and political impacts. We then examine the current regulatory context in Canada (at the time of writing, February 1, 2019) and highlight gaps.

We conclude with policy recommendations that would enable the Canadian government, social media platforms and journalism organizations to better understand and reduce the threats to democracy posed by disinformation and harmful speech. These are partly drawn from policies that other countries are pursuing. We call for a three-pronged policy framework: 1) greater enforcement of existing laws, 2) regulation to encourage and help social media platforms address abuses; and 3) improved civil society measures, especially by journalism organizations.

2. THE PROBLEM OF ONLINE DISINFORMATION

Concern about the threat to democracy posed by social media has increased dramatically in recent years, with evidence that false information and state-sponsored information operations were widespread during election campaigns in countries including France, Germany, Kenya, Ukraine, the United Kingdom (U.K.), and the United States (U.S.).² In particular, the 2016 U.S. elections alerted the world to the many ways that social media platforms could be used to undermine the quality of information and political discussion.

Since 2016, policymakers and researchers have shifted from focussing on “fake news” to concentrate instead on online “disinformation.”³ A report by

¹ Democratic Institutions, Government of Canada, “Safeguarding Elections”, February 5, 2019. Online: <https://www.canada.ca/en/democratic-institutions/news/2019/01/safeguarding-elections.html>.

² Communications Security Establishment, *Cyber Threats to Canada's Democratic Process* (Government of Canada, 2017); Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report* (House of Commons: United Kingdom, 2018); Kimiko de Freytas-Tamura, “As Kenya's Vote Nears, Fear That ‘Fake News’ May Fuel Real Bloodshed” (August 6, 2017) *The New York Times*. Online: <https://www.nytimes.com/2017/08/06/world/africa/kenya-election-kenya-tta-odinga.html>; Council of the European Union, *Conclusions of the Council and of the Member States on Securing Free and Fair European Elections* (Brussels, 2018). Online: <https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf>.

the European Commission's independent expert group explains that “fake news” is a problematic term for policy analysis for two reasons.⁴ First, some politicians and their allies use the term to dismiss unwelcome coverage, to attack legitimate news organizations, and to undermine press freedom. While there are legitimate and longstanding critiques of journalism and its gatekeeping functions, the cry of “fake news” ignores the complexity of these arguments. Second, the term does not adequately capture the complex problem of disinformation, which often is not entirely “fake” or false, and which often does not look like conventional news media content. Instead, disinformation includes complex blends of fact and fabricated information, manipulated images and videos, organized trolling, the use of automated accounts to amplify or silence certain messages, and much more. As a U.K. parliamentary committee report argued, “fake news” is “a poorly-defined and misleading term that conflates a variety of false information, from genuine error through to foreign interference in democratic processes.”⁵

The term “disinformation” focusses discussions on specific types of politicized and monetized information campaigns and how they might undermine democratic legitimacy. The European Commission defines disinformation as “verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.”⁶ This definition emphasizes intent. Political actors use disinformation techniques to knowingly deceive the public and cause public harms such as undermining confidence in the electoral process.

Forms of online disinformation that have been used in election campaigns include:

- The leak of hacked documents, possibly tainted with fake information.⁷

³ Wardle, Claire, and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making* (Strasbourg: Council of Europe, 2017). Online: https://firstdraftnews.com/wp-content/uploads/2017/10/Information_Disorder_FirstDraft-CoE_2018.pdf?x56713; Joshua Tucker *et al.*, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature* (Menlo Park, CA: The William and Flora Hewlett Foundation, 2018). Online: <https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf>.

⁴ High Level Expert Group on Fake News and Online Disinformation, *A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation* (Luxembourg: European Commission, 2018) at 10.

⁵ Digital, Culture, Media and Sport Committee, *supra* note 2.

⁶ European Commission, *Tackling Online Disinformation: a European Approach*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels, 2018) at 2-3.

⁷ Citizen Lab, “Tainted Leaks: Disinformation and Phishing with a Russian Nexus”, Citizen Lab, Munk School of Global Affairs (Toronto: University of Toronto, 2017); Chris Doman, “MacronLeaks — A Timeline of Events” (May 6, 2017) *AlienVault*.

- The circulation of false information about when, where, or how to vote, or other deceptive messaging that seeks to reduce voting activity.⁸
- False claims about political candidates and parties, from fabricated party platforms to conspiracy theories about people's involvement in criminal activities.
- Hyper-biased content with information that is framed or presented in ways that are intentionally deceptive.
- Memes and other media forms that promote false understandings of issues or individuals, but that are difficult to fact-check or otherwise disprove.
- Faked images, videos, or audio recordings.

Scholars do not yet agree on the reach and impacts of these forms of disinformation in elections, and there is very little research on these issues in the Canadian context.

Disinformation is not unique to digital media. However, social media platforms have introduced new vulnerabilities to disinformation into the information ecosystem.⁹ These new vulnerabilities have led to problematic communication techniques including:

- The use of bots to amplify messages or create false impressions of their popularity.¹⁰
- The use of fake accounts to increase the spread or credibility of false information.¹¹
- Ad buys, influencer marketing, and promoted posts that violate electoral regulations.¹²
- For-profit sites, including those which mimic news organizations, that attract visitors via engaging but false information to earn revenue from advertising or the sale of other products.¹³

Online: <https://www.alienvault.com/blogs/labs-research/macronleaks-a-timeline-of-events>.

⁸ Fruzsina Eordogh, "Pro-Trump Trolls Want You To Vote For Hillary Via Text (You Can't)" (November 3, 2016) *Forbes*. Online: <https://www.forbes.com/sites/fruzsinaeordogh/2016/11/03/pro-trump-trolls-want-you-to-vote-for-hillary-via-text-you-cant/>.

⁹ Derakhshan & Wardle, *supra* note 3; Chris Tenove *et al.*, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy*, Working Paper Series Vancouver, Canada: Centre for the Study of Democratic Institutions (University of British Columbia, 2018); Tucker *et al.*, *supra* note 3.

¹⁰ Samuel C. Woolley & Philip N. Howard, eds, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford: Oxford University Press, 2018).

¹¹ Philip N. Howard *et al.*, *The IRA and Political Polarization in the United States* Project on Computational Propaganda (University of Oxford, 2018).

¹² Young Mie Kim *et al.*, "The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook" 35(4) *Political Communication* 515-554, 2018.

¹³ Craig Silverman, "This Is How Your Hyperpartisan Political News Gets Made" (February 27, 2017) *BuzzFeed*. Online: <https://www.buzzfeed.com/craigsilverman/>

- Irresponsible content curation and dissemination, including social media algorithms that reward sensationalistic content.
- Adversarial attacks on algorithmic recommendation systems, including by click-bait farms and other means, that can badly skew search results, “trending” topics, and other forms of recommendation.¹⁴

Politicians and commentators have focussed on foreign attempts to influence elections through disinformation, particularly Russian government-backed operations. The Russian and Soviet governments have a long history of using disinformation on domestic and foreign populations,¹⁵ though so do other governments, including the U.S.¹⁶ Today, many governments use deceptive social media campaigns to advance their interests.¹⁷ Domestic groups may also use disinformation techniques to influence their own elections, which may require different policy responses than foreign interference. However, the same false messages may be spread by both domestic and foreign actors, with domestic actors either knowingly or unknowingly advancing the political objectives of foreign governments.¹⁸ For instance, in the 2016 U.S. election, Russia-backed actors hacked and leaked the private data of the Democratic Party and Hilary Clinton’s campaign team, but this material was then propagated by mainstream journalism organizations, fake news sites, Republican politicians, and interested citizens.

Some kinds of false and deceptive information already violate existing Canadian laws, as described below. However, addressing disinformation often requires difficult or even controversial judgments about truth, intent, and legitimacy of messages during election campaigns. Criminal laws targeting “fake news” raise serious concerns about the violation of rights to free

how-the-hyperpartisan-sausage-is-made; Craig Silverman *et al.*, “How A Canadian Yellow Vest Site Used Fake Accounts And Marketing Savvy To Monetize Outrage” (February 7, 2019) *BuzzFeed*. Online: <https://www.buzzfeed.com/craigsilverman/canada-yellow-vest-site-internet-marketer>.

¹⁴ Dipayan Ghosh & Ben Scott, *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet* (Washington, D.C.: New America Foundation; Shorenstein Centre, Harvard Kennedy School, 2018); Jonathan Goldsbie, “How The Far Right Spun The Toronto Van Attack As Islamic Terrorism” (April 24, 2018) *CanadaLand*. Online: <http://www.canadalandshow.com/far-right-spun-the-toronto-van-attack-as-islamic-terrorism/>.

¹⁵ Nicholas J. Cull *et al.*, *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it* (London School of Economics and Political Science, 2017); Marcus Kolga, *Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation* (Ottawa: Macdonald-Laurier Institute, 2019).

¹⁶ Dov H. Levin, “When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results” (2016) 60:2 *Int. Stud. Q.* 189.

¹⁷ Samantha Bradshaw & Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*, Working Paper (Oxford: Project on Computational Propaganda, 2018).

¹⁸ Tenove *et al.*, *supra* note 9. Yochai Benkler *et al.*, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford: Oxford University Press, 2018).

expression, and have primarily been used by countries with poor records on expression rights.¹⁹

3. THE PROBLEM OF HARMFUL SPEECH

We use the term “harmful speech” to refer to communication that is abusive, threatening, denigrating or that incites violence, and which may therefore undermine people’s full, free and fair participation in politics and political debates.²⁰ Harmful speech takes many forms on social media platforms. Examples include targeted harassment of individual Twitter users, hateful videos posted on YouTube or Facebook, and the unwanted exposure of individuals’ private information on Reddit.

We do not offer one static definition of harmful speech. Harm and harmful speech can take different forms and mean different things to different individuals and societies over time. Definitions should thus emerge from ongoing public discussion. However, commonly-recognized forms of harmful speech online include:

- Hate speech, which attacks a social group or members of a group based on qualities such as race, ethnicity, religion, nationality, sexual orientation, gender, or disability.
- Threats and intimidation that target individuals, which are often used against public figures such as politicians, journalists and activists. These include direct threats of violence or sexual assault, threats to spread false information, and threats to expose personal information or private contact details online (known as doxing).
- Co-ordinated and repeated harassment of individuals by multiple attackers or accounts, which can include offensive speech and memes, repeated insults, adversarial use of platform complaint processes, and the use of bots or fake accounts to flood their social media feeds. These and other techniques may be legal but can significantly undermine people’s abilities to communicate online.

These and other forms of harmful speech often overlap with disinformation, such as spreading false information about groups or individuals in order to discredit or denigrate them.

As with disinformation, harmful speech is used by foreign and domestic actors to advance political aims, and may in some cases be part of state-backed information operations. State-sponsored trolls (government employees or

¹⁹ Kate Lamb, “Cambodia ‘fake news’ crackdown prompts fears over press freedom” (July 6, 2018) *The Guardian*. Online: <https://www.theguardian.com/world/2018/jul/06/cambodia-fake-news-crackdown-prompts-fears-over-press-freedom>; Ruth Michaelson, “‘Fake news’ becomes tool of repression after Egypt passes new law” (July 27, 2018) *The Guardian*. Online: <https://www.theguardian.com/global-development/2018/jul/27/fake-news-becomes-tool-of-repression-after-egypt-passes-new-law>.

²⁰ This definition and many of the subsequent arguments draw on our previously-published report: Chris Tenove, Heidi J.S. Tworek & Fenwick McKelvey, *Poisoning Democracy: How Canada Can Address Harmful Speech Online* (Ottawa, ON: Public Policy Forum, 2018).

contracted firms) are widely engaged in “making death and rape threats, using bots and automated agents to amplify vitriolic attacks at scale, making accusations of treason or collusion with foreign intelligence agencies . . . and sowing acrimonious sexism.”²¹ Ideological communities and extremist groups also pursue coordinated campaigns of harmful speech. These include transnational alt-right groups, which promote stigmatization of people of different racial, ethnic, gender, and religious identities.²² Alongside governments and organized groups, many individuals create, target, and share harmful speech. Some do so with political intent, some to settle personal scores, and some do so occasionally, in response to major news events, including elections.

Harmful speech online not only has different creators; it also has different target audiences. Hate and abuse are sometimes directed at individuals or groups to cause them distress or are posted publicly for all to see. They may also be disseminated in semi-private or “dark” social media spaces, such as Facebook Groups, 4Chan sites, or WhatsApp groups. These methods are used by extremist and pro-hate groups (but also human rights activists in repressive countries) to build group identity and plan future actions. Researchers and law enforcement struggle to quantify the extent of such messaging, both because it may be hidden or encrypted, and also because it rarely provokes complaints to law enforcement officials or social media companies.

Canadian users appear to be exposed to large amounts of harmful speech on social media platforms. A 2016 survey found over one-quarter of people have been harassed via social media platforms, with higher rates among users who are young (under 34), or who identify as LGBTQ or a visible minority.²³ Journalism investigations have found Canadian actors spreading or seeking hateful content.²⁴ There are, however, serious shortcomings regarding data on Canadian experiences of harmful speech online. Surveys and quantitative analyses use very different definitions of harassment and other terms. Social media platforms like Facebook and Google release global transparency

²¹ Carly Nyst & Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns* (Palo Alto, CA: Institute for the Future, 2018) at 11.

²² Rebecca Lewis, *Alternative Influence: Broadcasting the Reactionary Right on YouTube* (New York: Data & Society Research Institute, 2018; Barbara Perry), “The threat of right-wing extremism” (September 13, 2017) *Policy Options*. Online: <http://policy-options.irpp.org/magazines/september-2017/the-threat-of-right-wing-extremism/>.

²³ Angus Reid Institute, *Trolls and Tribulations: One-in-four Canadians Say They’re Being Harassed on Social Media* (Vancouver, BC: Angus Reid Institute, 2016). In this survey, “harassment” ranged from being called offensive names to cyber-stalking and threats of violence.

²⁴ Alex Boutilier, “Rise of right-wing extremists presents new challenge for Canadian law enforcement agencies” (October 7, 2018) *The Toronto Star*. Online: <https://www.thestar.com/news/canada/2018/10/07/rise-of-right-wing-extremists-presents-new-challenge-for-canadian-law-enforcement-agencies.html>; Silverman *et al.*, *supra* note 13.

reports, revealing that they deal with several million pieces of hateful content each quarter. However, the data is often not broken down by country.

Harmful speech is not a problem that can simply be “solved.” Instead, Canada and other democracies need to engage in ongoing efforts to safeguard rights to free expression, thought and belief, as well as preventing harmful speech from disadvantaging individuals or groups based on race, national or ethnic origin, colour, religion, sex, gender expression, age, or mental or physical disability. Political speech in Canada has never been completely civil, but the frequency, scale, and ad-hoc enforcement of online communication have introduced serious new challenges to these longstanding issues in democratic participation.

4. WHAT THREATS DO DISINFORMATION AND HARMFUL SPEECH POSE TO DEMOCRACY?

Disinformation and harmful speech take diverse forms, are used by a range of actors, and target different individuals and groups. To address them will necessitate a complementary set of government policies and civil society actions. Doing so will require that their consequences are taken seriously. While disinformation may affect people’s knowledge about issues of health or personal finance, and harmful speech can have myriad social and mental health effects, they also pose distinct threats to the quality of elections. This section highlights threats that disinformation and harmful speech can pose to three core democratic goods.²⁵

First, democracy means that citizens have fair opportunities to participate in political activities, including voting, running for office, or contributing to political debates. Digital techniques have been used to undermine or diminish some people’s participation. For instance, people’s ability to vote may be compromised by false information about voting times and places, or falsehoods about candidates and party positions. Participation may also be undermined if individuals or groups are targeted with online threats, stigmatization, or harassment, which may create unfair obstacles to running for office or participating in public debates. Targeted groups often already face barriers to full political participation, including ethnic, racial, religious, or gender minorities.

Second, democracy requires robust public deliberation. Citizens need to put forward their concerns, insights, values, and interests; candidates must advance their platforms and respond to claims made by their opponents; and other domestic and foreign actors can weigh in with relevant views. Domestic and foreign actors have used fake news sites, political bots, targeted social media ads, and other techniques to spread false information, to exacerbate social conflicts, or through attempts to hijack the “agenda” of public discussion during a campaign (e.g. the strategically-timed leaking of candidates’ or parties’ private documents). There is also a growing concern about faked representations of candidates or government officials, including

²⁵ This analysis is primarily drawn from Tenove *et al.*, *supra* note 9.

fake audio and video, otherwise known as deep fakes. More broadly, trolling tactics and mass disinformation may undermine expectations of civility, reciprocity, authenticity, and other basic norms of democratic deliberation.

Third, fair elections require that institutions can effectively facilitate democratic processes and enforce rules. Actors have used digital techniques to interfere in the work of electoral commissions and other state agencies, to violate rules on campaign spending and foreign interference, and to attack or create unfair advantages for certain candidates, political parties, or third-party actors. Many institutions need to reformulate their policies to address digital interference in elections. For instance, electoral agencies need to evaluate paid advertising and unpaid amplification of political messages on social media that may violate laws on political spending or foreign communication; intelligence agencies must identify and respond to foreign influence operations; and political parties may need to develop codes of conduct to avoid becoming dupes of influence operations.

5. THE POLICY LANDSCAPE IN CANADA

Canada has both longstanding and recently-introduced policies to address online disinformation and harmful speech that may undermine elections. It must be recognized that, in many ways, the primary “regulators” of online disinformation and harmful speech — and therefore free expression — are not government bodies but the large social media platforms themselves. This happens primarily through content moderation.²⁶

(a) Regulatory Frameworks for Disinformation and Harmful Speech

Federal and provincial governments have developed several legal frameworks that can be used to address disinformation and harmful speech online.²⁷ These include:

Criminal law. Various forms of disinformation and harmful speech fall under the *Criminal Code*, including criminal harassment, defamatory libel, counselling suicide, uttering threats and intimidation. There are also criminal provisions against hate speech. Specifically, s. 318 and 319 impose criminal sanctions against anyone who intentionally promotes genocide or who incites hatred against groups identifiable by factors such as race, religion, and sex.

Human rights law. Multiple provincial and territorial human rights provisions prohibit the incitement of hate or group discrimination through

²⁶ Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven, CT: Yale University Press, 2018); David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (United Nations Human Rights Council, 2018).

²⁷ Jane Bailey, *Abusive and Offensive Speech Online: An Overview of Canadian Legal Responses Focusing on the Criminal Law Framework* (Law Commission of England and Wales, 2018).

public displays, broadcasts or publications. So, too, did s. 13 of the *Canadian Human Rights Act*, until it was repealed in 2013.

Civil litigation. Individuals can pursue civil litigation to seek redress for some forms of harmful speech, including defamation and the non-consensual disclosure of intimate images.

Regulatory/administrative law. Several federal, provincial, and territorial governments include offices or support units that might help address different forms of disinformation and harmful speech. For instance, Canada's Anti-Spam Legislation can be used against mass distribution of email, text, or other messages, and could arguably be expanded to address bots.²⁸ Privacy commissioners can address complaints and contribute to requests for service providers to remove content, such as the non-consensual disclosure of private information or intimate images.

Security and Intelligence. Canada's intelligence agencies, the Communication Security Establishment (CSE) and the Canadian Security and Intelligence Services (CSIS), have shown increasing attention to digital threats to election integrity.²⁹ These agencies and the RCMP are part of new task forces to monitor and potentially disrupt foreign interference.³⁰

Electoral law. The Canada *Election Act* was updated by Bill C-76, the "Elections Modernization Act" (2018), with provisions against knowingly making false or misleading statements about electors and voting processes, or about certain qualities of candidates (such as their citizenship and education, or whether they have been charged or convicted for breaking a law).³¹ The *Act* does not address harmful speech per se, but it does have provisions against undue influence by foreigners, including through spending by foreign third parties to influence election outcomes, which could be applied to disinformation campaigns or harmful speech from foreign entities.

Furthermore, Elections Canada has a mandate to address false information regarding where, when, and how people may vote, including on social media. The Chief Electoral Officer has announced that the agency will use social media monitoring tools to identify disinformation and respond to it.³²

²⁸ Fenwick McKelvey & Elizabeth Dubois, *Computational Propaganda in Canada*, Computational Propaganda Research Project Working Paper: Computational Propaganda Research Project (University of Oxford, 2017).

²⁹ Communications Security Establishment, *supra* note 2; Canadian Security Intelligence Service, *Who Said That? The Security Challenges of Modern Disinformation*, World Watch: Expert Notes Ottawa: Canadian Security Intelligence Service, 2018.

³⁰ Democratic Institutions, Government of Canada, *supra* note 1.

³¹ *Elections Modernization Act*, December 13, 2018 [*Elections Modernization Act*], s. 61, s. 481.

³² Charlie Pinkerton, "Elections Canada will use AI to fight disinformation on social media" (November 2, 2018) *The Star*. Online: <https://www.thestar.com/ipolitics/federal/2018/11/02/elections-canada-will-use-ai-to-fight-disinformation-on-social-media.html>.

(b) Social Media Regulation

These legal measures provide important means for governments and individuals to address some of the most egregious forms of disinformation and harmful speech. Effective use of these measures may, however, be limited by legal definitions, operational challenges, and obstacles to co-operation across different agencies.

Even if these legal measures were used more robustly, they would not adequately address disinformation and harmful speech on social media. They tend to be costly and difficult to enforce (particularly if the responsible party is hard to identify or resides outside of Canada), and they are slow and reactive — making them less suitable for addressing hate and harassment in the midst of an election campaign.³³ Finally, these measures are narrow and have a high threshold for action, focussed as they often are on individual or organizational culpability. This makes them inappropriate tools for addressing forms of disinformation and harmful speech that are problematic and widespread but that should not lead to individual legal sanction.

We therefore argue that disinformation and harmful speech online must also be addressed as an issue of media regulation and media standards. There is extensive regulatory policy regarding broadcasters and publishers in Canada. These include specific provisions that apply during election campaigns, to promote fairness in political parties' and candidates' ability to put forth their messages via news media, including access to airtime and opportunities to advertise. In addition, the Canadian Broadcast Standards Council has developed codes of conduct on issues including broadcasting ethics, depictions of violence, and unduly negative or stereotyped portrayals of social groups. The council ensures these codes are enforced, provides templates for complaints, and offers an appeals process. It also releases annual data on the number of complaints.

Social media platforms are not bound by comparable policies in Canada, in part because they do not neatly fit into Canadian policies on telecommunications, broadcasting, or publishing. The novelty and ambiguous status of social media platforms has challenged their regulation as media. We therefore argue in the next section that regulatory measures need to be developed to address the role social media platforms play in disseminating — and responding to — disinformation and harmful speech.

6. POLICY RESPONSES TO DISINFORMATION AND HARMFUL SPEECH

This final section suggests policy responses that could be used in a complementary fashion to address the risks that online disinformation and harmful speech pose to democratic elections. These actions build on or go

³³ Exceptions include Elections Canada's ability to respond to disinformation about voting processes, and the new government task forces to assess potential foreign interference and to publicize significant threats to election integrity during the writ period.

beyond existing responses in Canada. Our recommendations focus on threats to the quality and participatory opportunities of the information system, rather than on technically difficult but politically straightforward responses such as prosecuting violations of existing laws or improving cyber-security of candidates, political parties and electoral management bodies. The problems of disinformation and harmful speech for the information system are ecosystemic, and successful responses will involve multiple stakeholders and overlapping efforts. Policy responses must also safeguard freedom of expression, which is a core tenet of democracy. However, as Canadian jurisprudence and policy has long recognized, freedom of expression in a democracy is not best served by the absence of regulation on expression, but rather by policies that protect people’s “reasonable opportunity to speak and be heard” and each “voter’s ability to be adequately informed of all views.”³⁴

(a) Government Responses:

(i) Enforcing Existing Law on Illegal Content

Federal and provincial governments have many legal tools to address disinformation and harmful speech, particularly for holding to account individuals or organizations that violate existing laws. Greater commitment to using these tools, and better coordination in overlapping areas of action, is needed. Government and independent researchers also need to assess the impact of these legal measures on online communication during elections.

(ii) Addressing Deceptive Election-Related Messaging

In January 2019, the Canadian government announced a task force to monitor potential foreign interference during the election period. Government and independent researchers also need to assess the impact of these legal measures on online communication during elections.³⁵ It also announced the creation of a process, the “critical election incident public protocol,” by which government public servants could alert Canadians about foreign or domestic interference that might undermine the integrity of the federal election. There is also a new Digital Citizens Initiative to improve Canadians’ digital literacy. The effectiveness of these policies remains untested.

Recent initiatives in other democracies may provide additional comparison for how the Canadian government might minimize the impact of deceptive election-related messaging, while not constraining freedom of speech. In December 2018, after much heated debate, France promulgated a law against the manipulation of information during elections. This created a judicial process to prevent the spread of “objectively” false information during the three months prior to an election.³⁶ Some countries have created separate

³⁴ *Harper v. Canada*, 2004 SCC 34, [2004] 1 S.C.R. 827, at 829.

³⁵ Democratic Institutions, Government of Canada, *supra* note 1.

³⁶ Online: https://www.senat.fr/espace_presse/actualites/201806/lutte_contre_les_faus-ses_informations.html.

offices dedicated solely to dealing with new types of threats, rather than leaving it to the existing electoral management body. Australia established an electoral integrity assurance taskforce in June 2018, the first in the world dedicated to assessing cyberthreats to elections. In August 2018, the California governor approved the creation of an Office of Elections Cybersecurity to focus on countering social media campaigns that intend to confuse voters about voting processes or to discourage them from voting.³⁷

(iii) *Require Adequate Transparency from Social Media Companies*

As we argue in the section below, social media companies need to provide more information to Canadians about the content that is promoted, purchased, shared, and removed during election campaigns. The recent Bill C-76 requires social media companies to create repositories of political advertisements. However, as experts and civil society groups have pointed out, social media companies in other jurisdictions have failed to create advertising repositories that include all political advertising and that make accessible information in an adequate form for researchers and journalists to use.³⁸ The Canadian government should ensure that social media companies address these issues before, during, and after the coming federal election campaign.

Social media platforms are a new form of mass media and, as noted above, Canada does not yet have adequate policies to ensure that they will responsively and transparently address threats to democracy. We have therefore argued for the creation of a Moderation Standards Council.³⁹ This would be a multi-stakeholder body that would convene platforms, government representatives, and civil society organizations regularly to discuss content moderation, and pursue best practices when it comes to addressing issues including disinformation and harmful speech.

(b) Political Party Responses

Political parties themselves are key to improving communications integrity during a campaign. Canadian researchers Fenwick McKelvey and Elizabeth Dubois have suggested that political parties should develop voluntary codes of

³⁷ Assembly Bill No. 3075. Online: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB3075.

³⁸ Mozilla Foundation, “Open letter to Facebook” (February 2019). Online: <http://foundation.mozilla.org/en/campaigns/eu-misinformation/>. For problems with Facebook’s ad archive in the U.S. 2018 elections, see Jeremy B. Merrill, “How Big Oil Dodges Facebook’s New Ad Transparency Rules” (November 1, 2018) *ProPublica*. Online: <https://www.propublica.org/article/how-big-oil-dodges-facebooks-new-ad-transparency-rules>; William Turton, “We posed as 100 senators to run ads on Facebook. Facebook approved all of them” (October 30, 2018) *VICE News*. Online: https://news.vice.com/en_ca/article/xw9n3q/we-posed-as-100-senators-to-run-ads-on-facebook-facebook-approved-all-of-them.

³⁹ Tenove, Tworek & McKelvey, *supra* note 20; Fenwick McKelvey, Heidi J.S. Tworek & Chris Tenove, “How a standards council could help curb harmful online content” (February 11, 2019) *Policy Options*. Online: <http://policyoptions.irpp.org/magazines/february-2019/standards-council-help-curb-harmful-online-content/>.

conduct for digital campaigning.⁴⁰ Civil society groups created a pledge against forms of online disinformation in the 2019 European Parliament elections, which can be signed by political parties and candidates.⁴¹ While some might counter that voluntary codes are made to be broken, they offer important measures of accountability. In addition, research suggests that politicians who publicly commit to not disseminating false information appear to be less likely to do so.⁴² Another important issue is how parties acquire, use, share, and safeguard data about voters' data. The recent Bill C-76 requires that political parties have and publicize their policies on data privacy, but does not offer any clear standards or means of enforcement. However, a Canadian parliamentary committee, Canada's Privacy Commissioner, and many experts and civil society organizations have argued for clear and enforceable standards.⁴³

(c) Social Media Platform Responses

(i) *Transparency*

Unlike newspapers, broadcasters, or most online sites, content distributed by social media platforms may be targeted to specific audiences and effectively invisible to all others. This targeting is combined with uncertainty about how social media platforms and their algorithms choose to propagate some content or remove other content for violating their terms of service. As a result, it is very difficult to identify or challenge disinformation and harmful speech during election campaigns, or to study the impact of social media messaging on election outcomes. The widespread violation of laws during previous elections, most notoriously the U.S. 2016 federal election, makes it clear that social media companies cannot effectively monitor all content on their own. Enhanced transparency is critical. As noted above, Bill C-76 requires that social media platforms create a public repository of all political advertisements during campaigns, but it is currently up to social media companies to ensure that these repositories have sufficient specificity and accessibility to be truly useful to researchers and citizens. In addition, greater access by researchers to the content, targeting, and removals of content is also needed.

We therefore argue that social media companies should provide greater access to independent researchers, who could then investigate the tactics and

⁴⁰ Fenwick McKelvey & Elizabeth Dubois, "Toward the responsible use of bots in politics" (November 23, 2017) *Policy Options*. Online: <http://policyoptions.irpp.org/magazines/november-2017/toward-the-responsible-use-of-bots-in-politics/>.

⁴¹ Alliance of Democracies & Transatlantic Commission on Election Integrity, "The Pledge for Election Integrity" 2019. Online: <https://electionpledge.eu>.

⁴² Brendan Nyhan & Jason Reifler, "The Effect of Fact-Checking on Elites: A Field Experiment on U.S. State Legislators" (2015) 59:3 *American Journal of Political Science* 628.

⁴³ Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, Committee Report 17 (Ottawa, ON: House of Commons of Canada, 2018).

effects of political communication during elections. Facebook, in particular, needs to improve access to independent researchers, as it is the most-used platform by Canadian citizens and electoral campaigns, and there are serious obstacles to research of communication on Facebook and its ancillary platforms, Instagram and WhatsApp. The timing of data access is crucial. The timing here is crucial. The data must be accessible and openly collected during a campaign and before an election is decided. Real-time collection and research can ensure that winning parties don't dismiss concerns as coming from "sore losers." While improving access, social media companies also need to build in policies to protect researchers from exposing or exploiting the private data of users, whether intentionally or inadvertently.

(ii) *Election Contact Group*

The government might require companies to designate specific point people at social media and tech companies who would deal with the Canadian election. These people could act as a contact group to ensure that any issues reported by Canadian citizens or electoral officials are swiftly examined and resolved. Long in advance of the election, the Canadian government could also establish a procedure by which the companies would make public any attempts at interference, hacking, or exceeding limits on third party spending. This ensures that any disclosures do not seem politically motivated, because the procedures were agreed long before the writ period. As this article goes to press, the Minister of Democratic Institutions is currently in talks with social media companies and may be creating measures along these lines.⁴⁴

(d) Journalism Organization Responses

Media organizations remain the key method for informing much of the electorate. They can sometimes unwittingly spread disinformation or harmful speech. To bolster and preserve the freedom of journalism organizations, we suggest how organizations might consider voluntary changes in their practices of reporting on two types of coordinated and deliberate disinformation and harmful speech: *weaponized information* and *fake personae*.

(i) *Change Coverage of Data Leaks*

Weaponized information includes both leaking information and amplifying (dis)information designed to sow distrust or create discord. Journalists are key to foreign (dis)information campaigns based on leaked or hacked information dumps. These campaigns only succeed if journalists amplify the dumps by reporting on their contents. While a few people will explore the mass of information released in a data dump, the vast majority only hear about leaked or hacked information through traditional media organizations' reporting. It

⁴⁴ This led to a voluntary declaration by social media companies to protect democratic integrity. Democratic Institutions, Government of Canada, "Canada Declaration on Electoral Integrity Online" (May 27, 2019). Online: <https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html>.

is of course legitimate for journalists to report on whatever they like. But they may be serving other agendas by reporting on the contents of a data dump, especially if portions have been modified to manipulate readers.

One approach is to cover the story of the data dump itself, rather than its contents. French journalists took this approach when data from Macron's campaign was hacked and released just before the election in 2017. German journalists reported similarly about a data dump of politicians' sensitive information in late 2018. This informed the public but did not amplify potentially falsified content. This approach may also prevent future hacks because it helps to invalidate their purpose.

(ii) *Avoid Amplifying Fake Personae and Harmful Speech*

During the 2016 election campaign in the U.S., 32 out of 33 major American news organizations embedded tweets created by the Russian-funded Internet Research Agency, generally from social media profiles purportedly operated by "real Americans."⁴⁵ These outlets ranged from NPR and *The Washington Post* to BuzzFeed and Salon. Canadian media outlets must ensure that they are not similarly duped by verifying Twitter users' identity before posting their tweets, for example by speaking with a user on the phone.

Organizations can also embed social media posts more responsibly, for example by quoting tweets rather than embedding them. If news outlets embed tweets, they might consider cutting out the portion showing replies/retweets/favourites. It avoids providing a potentially inaccurate snapshot in time; it also avoids over-legitimizing tweets by providing social proof of the number of retweets or favourites, which themselves may be inflated by bots and fake accounts.

Still, news organizations often need to report on extreme or anti-democratic figures, such as neo-Nazis. In those cases, organizations might consider simple techniques to avoid further amplification. Don't link back to their tweets or posts; use a screenshot or quote them instead. Don't include their Twitter handle. Don't provide "share the name" or url of their websites. Ensure "non-follow tags" are enabled on news sites for those links so that any clicks don't register as hits for them.⁴⁶

(iii) *Consider How to Improve Fact-Checking Partnerships*

Facebook has partnered with independent fact-checking organizations to help it address misinformation and disinformation.⁴⁷ Fact-checkers can choose

⁴⁵ Josephine Lukito & Chris Wells, "Most major outlets have used Russian tweets as sources for partisan opinion: study" (March 8 2018) Columbia Journalism Review. Online: <https://www.cjr.org/analysis/tweets-russia-news.php>.

⁴⁶ For further suggestions on how to improve reporting practices, see: Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information" (March 23, 2018) *The German Marshall Fund of the United States*. Online: <http://securingdemocracy.gmfus.org/publications/responsible-reporting-age-irresponsible-information>.

⁴⁷ These partners get help from Facebook in identifying messages that are potentially problematic.

to examine these messages and — if they find evidence that they are false — Facebook will reduce their circulation, alert people about the potential problems with the information, or remove the messages entirely (if they violate the company’s terms of service). In 2018, Facebook partnered with AFP, which employs two Canadian journalists to focus on Canada-related content.⁴⁸

Despite the importance of establishing truth, fact-checking only addresses a small part of the problem. Many readers of the original story may not see the fact-check. While research about the effect of fact-checks continues, the latest studies indicate that fact-checks change the minds of only small percentages of readers. Finally, fact-checking partners have expressed concerns about their work with Facebook, including the lack of transparency about which content is flagged for them, how quickly the fact-check appears in users’ newsfeeds, and the effect of fact-checks. Researcher Mike Ananny concluded that “the partnership has a great deal of power, but is accountable neither among its own partners nor to outsiders.”⁴⁹ Fact-checking alone cannot solve disinformation issues. Rather, it must form part of a far broader effort to ensure that media platforms do not amplify disinformation.

(iv) *Rethink the Business Models of Journalism*

Many of the incentives to create click-generating articles (or clickbait) stem from the serious financial difficulties for many Canadian news outlets. There are grave concerns about the long-term viability of quality public journalism in Canada. Many local outlets have closed or substantially reduced their coverage; advertising revenue is plummeting; it is at present unclear what financial models can sustain journalism. To address some of these issues, a Public Policy Forum report co-authored by Taylor Owen and Ed Greenspon provided dozens of recommendations grouped into four main sections: rebuilding information trust and integrity; bolstering civic infrastructure; reforming the regulation of information markets; updating governance of data rights.⁵⁰ Some of these require legal reform or government support, such as the \$595 million assigned over the next five years to aid Canada’s media sector. More broadly, it will not work to double down on past models of journalism. Rather, we need to rethink how reporting works online and how to include more diverse voices in media to reform, rejuvenate, and revive news-making in Canada.

⁴⁸ Tessa Lyons, “Hard Questions: How Is Facebook’s Fact-Checking Program Working?” (June 14, 2018) *Facebook Newsroom*. Online: <https://newsroom.fb.com/news/2018/06/hard-questions-fact-checking/>; see also: <https://factcheck.afp.com>.

⁴⁹ Mike Ananny, “Checking in with the Facebook fact-checking partnership”, *Columbia Journalism Review* April 4, 2018. Online: https://www.cjr.org/tow_center/facebook-fact-checking-partnerships.php.

⁵⁰ Ed Greenspon & Taylor Owen, *Democracy Divided: Countering Disinformation and Hate Speech in the Digital Public Sphere*, The Shattered Mirror Series (Ottawa: Public Policy Forum, 2018).

7. CONCLUSION

Disinformation and harmful speech are not new problems for Canadian democracy, but dramatic changes to our information ecosystems in recent years have created new vulnerabilities to them. We have suggested a set of complementary policies by governmental and non-governmental institutions to help address these online threats to democratic communications, while retaining and bolstering free speech and a robust, free press. None of these policies require that government control the online space, censor it, or curtail free expression. Instead, they apply existing laws or propose multi-stakeholder solutions that will foster free and full participation, encourage robust democratic discourse, and ensure the fair application of rules in elections.