

ONLINE CULTURE SHIFT

Safer Platforms for Women in Politics

AUGUST 2019

PUBLIC POLICY FORUM

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES

PPF

ABOUT PPF

Good Policy. Better Canada. The Public Policy Forum builds bridges among diverse participants in the policy-making process and gives them a platform to examine issues, offer new perspectives and feed fresh ideas into critical policy discussions. We believe good policy is critical to making a better Canada—a country that's cohesive, prosperous and secure. We contribute by:

- Conducting research on critical issues;
- Convening candid dialogues on research subjects; and
- Recognizing exceptional leaders.

Our approach—called **Inclusion to Conclusion—**brings emerging and established voices to policy conversations, which informs conclusions that identify obstacles to success and pathways forward.
PPF is an independent, non-partisan charity whose members are a diverse group of private, public and non-profit organizations.

© 2019, Public Policy Forum
1400 - 130 Albert Street
Ottawa, ON, Canada, K1P 5G4
613.238.7858

ISBN: 978-1-988886-71-8

ppforum.ca

@ppforumca

WITH THANKS TO OUR PARTNERS

This project has been supported by Women and Gender Equality Canada

Women and Gender Equality Canada
Femmes et Égalité des genres Canada

THANKS TO OUR EVENT PARTNERS

TELUS the future is friendly®

INFORMED OPINIONS ...is amplifying women's voices

equal voice

Government of Canada
Gouvernement du Canada

AUTHORS

Katherine Feenan
Policy Lead, Public Policy Forum

Kathleen Donovan
Research Assistant, Public Policy Forum

ACKNOWLEDGEMENTS

Thank you to **Aspa Kotsopoulos**, PhD, Senior Policy Analyst for Women and Gender Equality Canada for her assistance in helping to complete this important research project.

TABLE OF CONTENTS

Executive Summary 4

Introduction 5

Current Policies and Frameworks 7

- European Union 1
- Germany 3
- Australia 3
- Bolivia 5

Short Term: Stronger Internal Mechanisms and Policies 16

- Leadership from Political Parties 7
- Support Organizations Building Resilience & Empowering Women to Run for Office 17

Medium Term: Strong Laws to Address and Deter the Cyber-Harassment of Women 19

- Better Prepare and Equip Law Enforcement 19
- Opportunities for Technology Companies 20
- Enhance Media Standards and Regulation 14

Long Term: Social and Cultural Change 14

Conclusion 17

Appendix: Solutions to Cyber-Harassment Aimed at Women in Political Life: Agenda 19

EXECUTIVE SUMMARY

Women engaged in political life benefit from using social media. But characteristics of these platforms—specifically the ease of communication, high volume of interactions and anonymity—can lead to negative outcomes including cyber-harassment and the spread of misinformation, disinformation and harmful gender tropes.

On Feb. 19, 2019, the Public Policy Forum hosted a panel and roundtable discussion on strategies to address the troubling phenomenon of cyber-harassment of women in political life. The ideas and experiences highlighted during the event are integrated throughout this report.

Although there is no single silver-bullet solution, PPF, with support from Women and Gender Equality Canada, has established a clear framework of short-, medium- and long-term actions required to facilitate lasting social and cultural change.

Short-term actions include:

- requiring political parties to train all campaign team members on codes of conduct and anti-harassment policies; and
- providing government resources and financial support to organizations whose goal is to increase women's participation in politics, including ones providing digital resilience and bystander training.

Medium-term considerations should include the implementation of stronger laws and standards to address and deter the cyber-harassment of women, such as:

- improving law enforcement through consistent cyber-related legislation, training and resource allocation, and opportunities to leverage and develop institutional expertise; and
- assisting and giving incentives to technology companies to implement changes to their platforms and adopt standards that prevent cyber-harassment online.

The internet is a relatively new phenomenon. Misogyny and violent harassment, however, are not. While society tries to catch up to the changes brought about by the internet—specifically its ability to facilitate and amplify harmful behaviour—real and lasting change will occur only through social and cultural shifts occurring over the long-term.

Long-term change requires:

- agreed-upon language that defines online harassment and violence in order to tackle it through law enforcement;
- improvements in data collection to better understand the nature and extent of the problem; and

- a focus on gender equality in education to shift attitudes towards women in politics.

The women who choose to run for political office have views from across the political spectrum, advocating for a range of issues. Cyber-harassment of women is neither a partisan nor a gender issue. It is everyone's problem and, in turn, everyone's responsibility to solve.

INTRODUCTION

Social media and technology platforms have changed political life tremendously. Candidates, political parties and constituents now access a range of tools that allow for greater interaction and debate. Individuals can more easily share concerns and opinions with their representatives, and elected officials can access a vast network of volunteers and campaigners who are politically active online.

These platforms act as connectors and broadcasters, while also amplifying the messages of a greater diversity of political candidates. For example, during Alexandria Ocasio-Cortez's U.S. congressional campaign, a media production company discovered her unique story on Facebook and contacted her via Twitter direct message to see if she would be interested in creating a short video to promote her candidacy. The video went viral.[1] In Canada, Naheed Nenshi's 2010 Calgary mayoral campaign relied heavily on social media, which ultimately helped elect Canada's first Muslim mayor. Former Executive Director of Equal Voice, Nancy Peckford, said it was because of Facebook's ability to put her in touch with her community, and help her build a network of potential volunteers, that she won her North Grenville, Ont., mayoral campaign.

While women engaged in political life benefit from using social media, characteristics of these platforms can and do produce negative outcomes. The ease of communication, high volume of interactions and anonymity facilitated by technology platforms can lead to the spread of misinformation, disinformation and harmful gender tropes. A recent Inter-Parliamentary Union report pointed to social media as "the number one place in which psychological violence—particularly in the form of sexist and misogynistic remarks, humiliating images, mobbing, intimidation and threats—is perpetrated against women parliamentarians."[2]

As the National Democratic Institute pointed out in its #NotTheCost initiative, online platforms provide harassers with confidence, anonymity and access to networks where trolls can overwhelm candidates with negative messages. As an example, a former councillor for the London Borough of Newham in the U.K., Seyi Akiwowo, was overwhelmed by online trolls following her speech at a 2016 European Parliament Youth Event. This experience influenced her decision to leave elected office and, instead, advocate for an end to online abuse.

[1] Remnick, D. 2018. Alexandria Ocasio-Cortez's Historic Win and the Future of the Democratic Party. The New Yorker.

[2] Filion, B. 2016. Sexism, harassment and violence against women parliamentarians. Inter-Parliamentary Union.



Panelists Sandra Pepera, Kathy Macdonald, and Seyi Akiwowo. Feb. 19, 2019. PPF

The public scrutiny endured by women in political life, from all sides of the political spectrum, has always been decidedly harsher than commentary directed at their male counterparts. Politics is traditionally a male-dominated space and the advent of the internet, and the cyber-harassment[3] it facilitates, amplifies barriers to female participation. Moreover, women from already marginalized groups are at even greater risk of violence—cyber or otherwise. Citing the murder of Honduran community and Indigenous activist Berta Cáceres, United Nations Special Rapporteur Dubravka Šimonović stated: "If you are young, poor, and geographically isolated, you are at extreme risk of experiencing [gender-based violence] because of your political engagement in your group and community."[4] Further intersecting factors of identity—including, but not limited to, race, sexual orientation, gender identity and economic status—only increase barriers to engaging in political life.

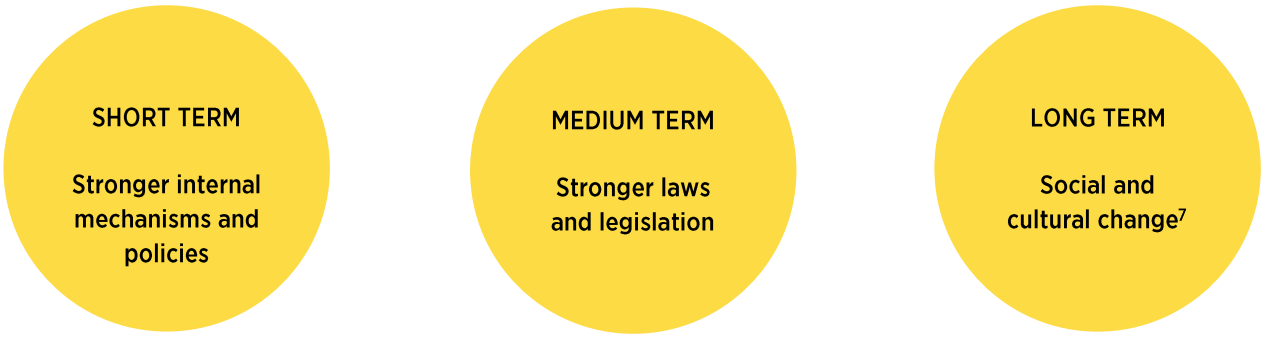
> **"If you are young, poor, and geographically isolated, you are at extreme risk of experiencing [gender-based violence] because of your political engagement in your group and community."[5]**
>
> - United Nations Special Rapporteur Dubravka Šimonović

[3] Terminology pertaining to this form of harassment has been and continues to be debated; however, for the purpose of this report, the umbrella term of 'cyber-harassment' is used to describe online behaviours directed at women in politics aimed to intimidate, dominate and/or exclude.

[4] United Nations Human Rights: Office of the High Commissioner. 2016. "Stop violence against women in politics" urges the Special Rapporteur on violence against women, its causes and consequences.

[5] Ibid.

On Feb. 19, 2019, the Public Policy Forum hosted a panel and roundtable discussion on strategies to address the troubling phenomenon of cyber-harassment[6] of women in political life. Although no silver bullet solution was identified, the discussion helped guide the creation of a clear framework of short-, medium- and long-term actions required to facilitate lasting social and cultural change. Based on the ideas and experiences highlighted during the event, and supplemented by research, we have created the following framework:



Short-term requirements for change are opportunities that can be put into action within the next year and allowed to progress. Medium-term requirements for change demand legislative efforts and therefore may take longer to implement—around three to five years. Long-term requirements point to a need for greater societal change, which only happens gradually—likely taking a decade or more. The opportunities for change outlined in this report are by no means exhaustive, but are intended to offer various approaches to bring about solutions to the cyber-harassment of women in politics.

CURRENT POLICIES AND FRAMEWORKS

Cyber-harassment of women in politics is not unique to Canada. It is prevalent across global jurisdictions, and, in turn, has prompted unique and innovative policy solutions. The European Union, Germany, Australia and Bolivia offer examples of compelling strategies to combat cyber-harassment of women.

In 2018, the Government of Canada vowed to help lead the fight against sexual and gender-based violence. Understanding how Canada has traditionally dealt with cyber-harassment and learning how other jurisdictions are dealing with this problem helps us to better advance solutions.

---

[6] Unwanted sexually explicit emails or other messages; Offensive advances in social media and other platforms; Threat of physical or sexual violence; Hate speech — meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and/or other traits (such as sexual orientation or disability); Any other online conduct meant to harm (e.g. cyberbullying, doxing, revenge porn).

[7] These three areas requiring change were identified in a Tweet by Jessica Roland, Senior Associate, Policy and Advocacy at Women Deliver. They were voiced during a roundtable session March 12, 2019, at the UN's 63rd session of the Commission on the Status of Women by Gabriela Cuevas Barron, Mexican Member of Parliament and President of the Inter-Parliamentary Union.

Canada

- **Canadian Criminal Code.** Cyber-harassment of women in politics could meet the threshold of several offences under the Canadian Criminal Code, including:
    - criminal harassment;
    - uttering threats and intimidation;
    - mischief in relation to data;
    - unauthorized use of computer;
    - identity fraud;
    - extortion;
    - false messages;
    - indecent or harassing telephone calls;
    - counselling suicide;
    - incitement of hatred; and
    - defamatory libel.8

  Unfortunately, the nature of cyber-harassment, and cyber-based crime in general, makes enforcing these laws extremely difficult. A significant challenge to using the Criminal Code as a regulator of cyber-harassment is the high standard of proof associated with criminal cases. Moreover, many women are reluctant to report their experiences fearing further harassment, re-traumatization, and loss of anonymity.

  A further problem with the Criminal Code as a regulator of cyber-harassment is that these crimes tend to cross jurisdictions. Online platforms may be hosted, operated and accessed in different jurisdictions than where the cyber-harassment occurred. Working across multiple international jurisdictions makes prosecution extremely difficult at best—and impossible at worst—due to a range of issues, including differences in laws across borders, lack of extradition agreements, and complex international relationships.

- **Court rulings on hate speech.** Debates on social media regulation, particularly on cyber-harassment and hate speech, often derive from interpretations of freedom of expression and whether restrictions are appropriate. Canadian legal precedent strongly indicates freedom of expression is not absolute and may be restricted to facilitate the protection of other fundamental rights and freedoms. In two landmark decisions in 1990[9], the Supreme Court of Canada concluded hate-motivated content presents "a serious threat to society."[10]

  In 2013, the Supreme Court of Canada reaffirmed this position by ruling that hate speech restrictions feed into the broader objective of addressing all forms of discrimination. These legal decisions indicate that citing freedom of expression to justify cyber-harassment is not a compelling argument

[8] Public Safety Canada. What are the potential legal consequences of cyberbullying?

[9] Canada Human Rights Commission v. Taylor. (1990) 3 S.C.R. 892.; R v. Keegstra. (1990) 3 S.C.R. 697.

[10] Ibid.

in Canada. Unfortunately, there is still significant ambiguity about how best to enforce reasonable restrictions on freedom of expression when violations occur online.

> **"Hate propaganda presents a serious threat to society… eroding the tolerance and open-mindedness that must flourish in a multicultural society which is committed to the idea of equality."**[11] – Supreme Court of Canada (1990)

- **Charlevoix commitment to end sexual and gender-based violence, abuse and harassment in digital contexts.** The Government of Canada recently vowed to become a global leader in cybersecurity, reaffirming this at the 2018 G7 meeting in Charlevoix in the form of a Commitment to End Sexual and Gender-Based Violence, Abuse and Harassment in Digital Contexts. The Inter-Parliamentary Union has recognized Canada for its efforts to address the issue by instituting both a parliamentary code of conduct and a complaints procedure.[12]

  Given the government's public commitment to address gender-based violence (GBV), as well as its current focus on workplace harassment and diversity and inclusion (e.g. Gender-Based Analysis (GBA+)), this is an opportune moment to advance dialogue on the impacts of cyber-harassment on women in public life. Good governance and healthy democracy cannot take place without the inclusion of women's perspectives in political discourse.

European Union

- **Istanbul Convention.** This Council of Europe Convention aimed at combating violence against women and domestic violence defines violence against women as "physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life."[13] This definition of violence against women allows for several substantive criminal law provisions pertaining to conduct in online spaces. For example, parties to the convention are required to take necessary legislative measures to protect women from psychological violence, stalking and sexual harassment—all of which have the potential to occur online.

  Once ratified by state governments, the Istanbul Convention is legally binding and government legislatures are obligated to implement provisions. To aid implementation, the Council of Europe has established GREVIO, an independent body responsible for monitoring the implementation and

[11] Ibid.

[12] Filion, B. 2016. Sexism, harassment and violence against women parliamentarians, p. 9. Inter-Parliamentary Union.

[13] Council of Europe. Istanbul Convention, CETS 210.

enforcement of the convention. It has already carried out baseline evaluations of Albania, Austria, Denmark, Monaco, Montenegro, Portugal, Sweden and Turkey, with the intention of providing constructive feedback on implementation processes. GREVIO has emphasized that the cyber-harassment of women should "be seen as a continuum of offline violence as a means to maintain women in an inferior position in the digital sphere and in real life."[14]

The Istanbul Convention is currently ratified by 34 member states and has been signed by 11 others.[15] Five years after the convention's entry into force, the Parliamentary Assembly of the Council of Europe is mostly satisfied with its impact.[16] In a memorandum on the convention's effectiveness, Rapporteur Zita Gurmai stated: "The first and foremost achievement of the Istanbul Convention is having lifted the shroud of silence that surrounds violence against women and domestic violence. The Convention sends out a clear message that violence against women and girls is not an unavoidable fact of life [that] they have to tolerate because they are women."[17] Furthermore, the President of GREVIO, Feride Acar, confirmed the convention has resulted in the introduction of new criminal offences, the modification of law provisions, and the stepping up of support services for women and girls.[18] Specific examples of actions taken by state parties were published in Gurmai's memorandum, The Istanbul Convention on violence against women: achievements and challenges.

Cyber-harassment of women is "a continuum of offline violence [and] a means to maintain women in an inferior position in the digital sphere and in real life."[19]

- **Budapest Convention**. This Council of Europe Convention on Cybercrime has several substantive provisions pertaining to cyberviolence. It criminalizes acts that both directly result in violence and that may facilitate violence. It is seen as complementary to the Istanbul Convention addressing violence against women and domestic violence. Like the Istanbul Convention, the Budapest Convention is binding, but has traditionally served as a guideline for states developing

[14] Council of Europe, Cybercrime Convention Committee. 2018. Mapping study on cyberviolence.

[15] Parliamentary Assembly. 2019. The Istanbul Convention on violence against women: achievements and challenges. Council of Europe.

[16] Parliamentary Assembly. 2019. The Istanbul Convention on violence against women: achievements and challenges. Council of Europe.

[17] Ibid.

[18] Ibid.

[19] Council of Europe, Cybercrime Convention Committee. 2018. Mapping study on cyberviolence.

comprehensive national legislation against cybercrime and as a framework for international co-operation between state parties. An outstanding problem for both conventions is enforcement.

Germany

- **Netzwerkdurchsetzungsgesetz (NetzDG) Law.** In June 2017, the German government passed a law requiring social media companies to remove harmful and illegal materials from their platforms within 24 hours or for "complex cases" within a week. Online platforms failing to comply risk fines up to €50 million. Companies receiving an excess of 100 complaints per year are required to publish reports articulating steps they have taken to address the problem.

  The NetzDG Law has been heavily criticized for undermining freedom of expression. Under tremendous time pressure, and out of an abundance of caution, many companies choose to remove legitimate expressions of opinion rather than face the possibility of significant government fines. U.K. human rights organization Article 19 cautioned: "The likelihood of Social Networks being over-vigorous in deleting or blocking content is compounded by legal uncertainty pervading the Act.... it is likely to create an environment wherein lawful content is routinely blocked or removed as a precaution."[20] Moreover, international human rights bodies have also voiced concerns this law could act as a model for more authoritarian regimes to repress online speech.[21]

  The law certainly caught the attention of technology companies, and harmful content on three major digital platforms (Google, Facebook and Twitter) is being removed at increased speed. Moreover, Facebook alone hired an additional 1,200 content moderators to scan harmful content flagged by German users.[22]

Australia

- **National Plan to Reduce Violence against Women and their Children 2010-2022.** This plan was released in 2011 and aims "to connect the important work being done by all Australian governments, community organisations and individuals to reduce [violence against women]."[23] The plan will be implemented over a 12-year period, but is divided into a series of three-year action plans that include clearly articulated priorities. Australian governments have agreed to prioritize these "foundations of change"[24], including improving female representation in the workforce, integrating

[20] Article 19. 2017. Germany: The Act to Improve Enforcement of the Law in Social Networks.

[21] Tworek, H. and Leerssen, P. 2019. An Analysis of Germany's NetzDG Law. Transatlantic Working Group.

[22] Bennhold, K. 2018. Germany acts to tame Facebook, learning from its own history of hate. The Independent.

[23] Government of Australia. 2011. National Plan to Reduce Violence Against Women and their Children.

[24] Council of Australian Governments. National Plan to Reduce Violence against Women and their Children: First Action Plan 2010-2013.

systems to share relevant information, improving data collection and establishing consistent collection standards, and tracking performances regarding implementation.

Because this plan is still being implemented, its long-term success is difficult to assess. Nevertheless, the plan has resulted in some clear instances of positive change. For example, the first action plan resulted in the creation of Australia's National Research Organisation for Women's Safety and has led to agreements between governments to establish a National Data Collection and Reporting Framework to build a better understanding of the prevalence and forms of violence against women. Under the plan, the Australian Bureau of Statistics would conduct a national Personal Safety Survey every four years.[25]

- **Office of the eSafety Commissioner.** The Australian Government established the Office of the eSafety Commissioner to receive complaints of cyber-harassment, oversee the removal of illegal content, and combat image-based abuse. The commission is also responsible for educating the Australian public about online safety and responsible digital citizenship.

  The Australian eSafety Commissioner has also been collaborating with technology platforms on initiatives to combat online behaviour that could be characterized as gender-based violence. For example, the commission has partnered with Facebook and victims' advocacy organizations on an initiative aimed at preventing the sharing of non-consensual intimate images (e.g. "revenge porn"). In this pilot program, individuals can proactively and securely submit images to Facebook to create a digital fingerprint preventing the images from being re-shared. The success and further implementation of this program is still being considered.

  The work of the eSafety Commission has resulted in some promising outcomes regarding the online safety of women. In 2016, it launched an eSafetyWomen initiative aimed at empowering women to manage technology risks and abuse. Its tactics to achieve this objective include initiating awareness-raising social media campaigns, offering training for frontline workers and providing resources and how-to videos for women active in online spaces.[26] In 2017-18, the website received over 50,000 unique visits.[27]

  In addition, in 2018, the commission launched another pilot program, called Women Influencing Tech Spaces, "to protect and promote women's voices online." Drawing on the experiences of women who have been cyber-harassed, this program aims to educate the Australian public and reframe the issue of cyber-harassment "not as a women's issue—but rather a societal issue that

[25] Council of Australian Governments. 2014. Progress Review of the First Action Plan to Reduce Violence against Women and their Children 2010-2022.

[26] Government of Australia. 2018. Annual Reports: Australian Communications and Media Authority and Office of the eSafety Commissioner.

[27] Ibid.

disproportionately affects women."[28] The website for this program includes resources on how to combat cyber-harassment, online safety tips, and resilience training and techniques.[29]

> **Cyber-harassment should be viewed "not as a women's issue—but rather a societal issue that disproportionately affects women."[30]**

Bolivia

- **Law against Harassment and Political Violence against Women**. After the murder of Ancoraimes town councillor Juana Quispe in 2012, Bolivia's legislative assembly passed a law prohibiting harassment and violence against women participating in political life.[31] The law carries with it a two- to five-year prison sentence for anyone who "pressures persecutes, harasses or threatens an elected woman or those exercising public functions."[32] In addition, anyone found guilty of "practising physical, psychological or sexual aggression"[33] is subject to penalties of three to eight years in prison.

  UN Women representative in Bolivia, Carolina Taborga, called this law "a model for other nations"; however, cultural and systemic issues have marred its effectiveness. Despite having high rates of female representation in political office, violence against women remains a problem and attacks against female politicians continue to rise. In 2015, more than 80% of female councillors reported experiencing at least one case of violence or political intimidation in office, most often carried out by their political rivals or peers.[34] Women coming forward often suffer retaliation in the form of false allegations of misconduct, withholding salary and physical violence. Others drop complaints due to challenges navigating a male-dominated legal system with little interest in their cases.[35]

  Although Bolivia's attempt at legislation to protect female elected officials does have flaws, it serves as a model, particularly in Latin America where rates of gender-based violence are high.

---

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] UN Women. 2012. Bolivia Approves a Landmark Law against Harassment of Women Political Leaders.

[32] Ibid.

[33] Ibid.

[34] Farthing, L. 2016. Despite Legal Protections, Violence Against Women is Spiking in Bolivia. World Politics Review.

[35] Flores, P. 2018. As women's roles expand in Bolivian politics, so do attacks. AP.

Key Themes from the Multi-jurisdictional Scan

Dominant themes arising from this multi-jurisdictional scan pertain to enforcement mechanisms, collaboration with technology companies and education initiatives.

1. **Enforcement mechanisms.** Enforcement remains one of the most significant challenges to addressing harmful and/or illegal behaviours in online environments. International conventions (e.g. the Istanbul and Budapest conventions) provide useful guidance and frameworks for amending domestic legislation, however, they lack coercive enforcement mechanisms. Similarly, changes to domestic legislation are ineffective without an accompanying shift in societal culture, particularly amongst law enforcement and within legal structures.
2. **Collaboration with technology companies.** Strategies yielding the most positive outcomes almost always included collaboration and trust-building initiatives between governments and technology companies. When overly coercive legislation is developed (as seen in Germany) technology companies may resort to overzealous interpretation and removal of potentially problematic speech, with poor implications for freedom of expression. Better outcomes appear to arise from collaborative initiatives.
3. **Education initiatives on gender equality.** As seen in Bolivia, laws and legislation are ineffective if enacted in isolation from cultural change. Lasting solutions to the harassment of women in politics require strategies that challenge norms, behaviours and stereotypes that perpetuate harmful narratives of who deserves to participate in public life. Education initiatives that articulate the benefits of gender equality can play an enormous role in shifting cultural narratives about who belongs in politics.

The key takeaways from this multi-jurisdictional scan inform the short-, medium-, and long-term actionable opportunities discussed in the next section.

THE WAY FORWARD

SHORT-TERM STEPS: STRONGER INTERNAL MECHANISMS AND POLICIES

Leadership from Political Parties

For some, resilience in the face of cyber-harassment may come easy. Not all are so lucky. Many women elected to office, regardless of their career path, say they were unprepared for the scrutiny and harassment they endured. Moreover, political staffers are equally impacted by cyber-harassment as they often play an intermediary role between elected officials and their online harassers. In other cases, staff become the trolls themselves.[36] Therefore, political parties should ensure candidates, elected officials, staff and bystanders are prepared for harassment—both online and otherwise.

- **Protection mechanisms and party structure.** The #MeToo movement has made political parties aware of the need to provide all of those engaged in political campaigns with behavioural guidelines. Over the short term, political parties need to develop internal mechanisms and policies to strengthen their ability to prepare, educate and support volunteers, staff, candidates and elected officials who face the effects of online harassment. Political parties should also have transparent mechanisms to deter and address issues of online misconduct. This should include basic security measures (e.g. security cameras and panic buttons in campaign offices) should online harassment turn violent.
- **Mandatory digital resiliency training.** In the run-up to an election, political parties should provide digital resilience and online interaction training to their candidates and campaign staff to ensure workers understand how to manage and cope with online harassment. Training should also be available for political staff, who often serve as buffers between elected officials and their harassers. Finally, bystander training should be implemented for those working around political candidates and staff to ensure preparedness for online harassment.
- **Standardized codes of conduct.** Political parties should consider making all campaign participants—following the completion of training exercises—sign a general code of conduct that includes stipulations around online harassment. Parties should consider openly displaying the codes of conduct, and those failing to meet the standards outlined should have membership revoked.

  Codes of conduct for political assemblies are also in the works in many jurisdictions. The Inter-Parliamentary Union has emphasized the importance of codes of conduct[37] and, according to two

[36] Baines, R. and Whitson, R. 2018. Senior Liberal staffer Martine Haley resigns after election trolling. ABC News.

[37] Filion, B. 2016. Sexism, harassment and violence against women parliamentarians, p. 9. Inter-Parliamentary Union.

IPU representatives interviewed for this project,[38] the organization has been monitoring the implementation of these documents among member states.

- **Adopting anti-harassment policies**. In 2017, former Canadian Parliament political staffer Beisan Zubi published an article listing reasons why women in politics often stay silent on allegations of harassment. Her reasons ranged from "because everyone [already] knew" to "because [the perpetrator] worked for my party."[39] In the wake of the #MeToo movement, stories like this one make it clear that political parties are failing to create environments for women to engage safely in political life.

  Political parties should work to improve and actively enforce anti-harassment policies to protect female candidates, elected officials and staff from harassment, both online and otherwise. Outlining policies and guidelines will ensure that all involved before, during and after campaigns are aware of the impact of their online presence and understand the parameters of appropriate conduct. Individuals that breach anti-harassment policies should be expelled from their political caucus and turned over to police when their conduct meets and exceeds the threshold of criminal conduct.

Support Organizations Building Resilience & Empowering Women to Run for Office

While, for some, developing resilience to cyber-harassment may come easily, others require guidance to empower, equip and mobilize. Moreover, intersecting factors of identity, which significantly impacts the severity and volume of harassment individuals experience, may also impact resiliency. Organizations active in this space play an important role in empowering women from diverse backgrounds to overcome barriers to political life created by cyber-harassment.

- **Training and mentorship programs.** NGOs have been crafting tools to assist, build and encourage the confidence of women and marginalized individuals to protect themselves while voicing their opinion online and offline. Governments should work to improve co-ordination with NGOs, not-for-profits and the corporate sector on prevention of cyber-harassment.
- **Resources and funding.** In Canada, the House of Commons Standing Committee on the Status of Women (FEWO) published an April 2019 report titled "Elect Her: A Roadmap for Improving the Representation of Women in Canadian Politics" that recommends greater support for organizations involved in "the political engagement of diverse groups of women," as well as those providing

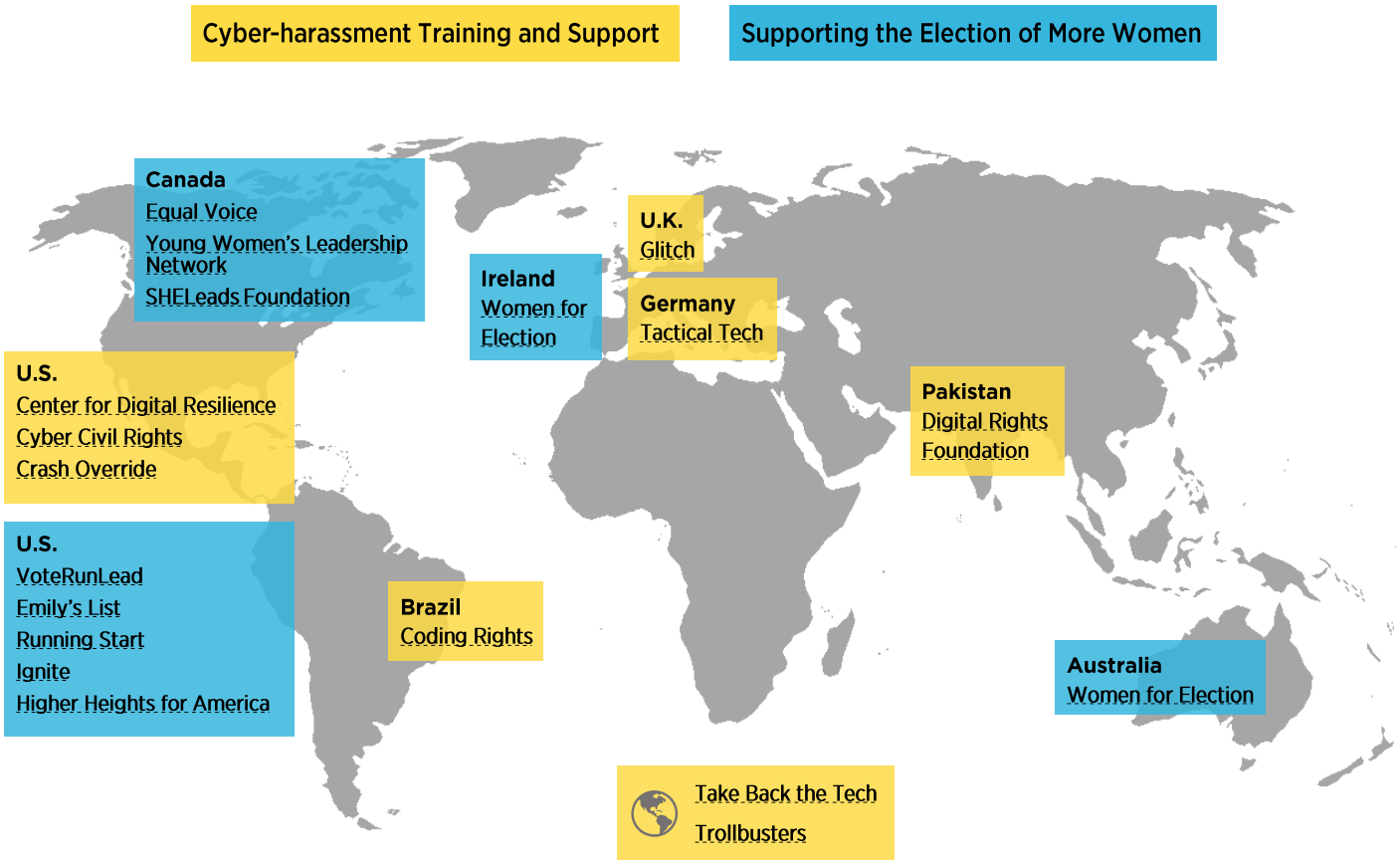
[38] Interview with Hon. Paddy Torsney, Permanent Observer to the United Nations, Head of the New York Office at Inter-Parliamentary Union, and Brigitte Filion, Programme Officer (Gender Equality) on June 24, 2019.

[39] Beisan Z. 2017. Here's why I never reported sexual harassment while working in Parliament. Vice News.

"relevant training… for women interested in seeking elected office."[40] In order to continue their important work in this space, organizations require sufficient funding.

SUPPORTING WOMEN IN POLITICS

Examples and links to organizations either providing cyber-harassment training or supporting women seeking to engage in public life:



Additionally, several international organizations and NGOs, funded by governments and private donations work internationally to empower and encourage diversity in politics. They include:

- The Association for Progressive Communications
- The National Democratic Institute

[40] House of Commons Standing Committee on the Status of Women (FEWO). 2019. Elect Her: A Roadmap for Improving the Representation of Women in Canadian Politics, p.6.

This report was published as a first step to increasing female representation at all levels of government in Canada. Females currently account for only 35 percent of all legislators. The report lays out 14 key recommendations to achieving this objective.

- International Republican Institute
- Atalanta
- The Inter-Parliamentary Union
- Hollaback!

MEDIUM-TERM STEPS: STRONG LAWS TO ADDRESS AND DETER THE CYBER-HARASSMENT OF WOMEN

Better Prepare and Equip Law Enforcement

Current studies indicate most police forces are not adequately educated about or trained to respond to forms of abuse occurring online.[41] Even in countries where laws regulating online speech exist, responses to online harassment are inconsistent and criminal convictions are few. For example, in Germany, only 2% of cyberstalking cases brought before police services resulted in convictions.[42] This problem is compounded by low rates of reporting from women who fear their experiences of gender-based violence will not be taken seriously or handled sensitively.

Moreover, the borderless nature of online platforms—specifically the likelihood they are hosted, operated and accessed in different jurisdictions—presents significant challenges for regulation and enforcement. Nevertheless, while inconsistent cyber-legislation presents challenges to law enforcement, opportunities exist to improve responses to incidents and to support of victims.

- **Improve training and awareness within law enforcement**. Law enforcement requires training to facilitate a better understanding of cyber-related crime. Although recognition of this need exists, jurisdictions have yet to fully realize requirements for policing harassment and violence online. In 2016, former California Attorney General Kamala Harris announced an initiative to devote greater time and resources to dedicated training programs for law enforcement.[43] Developing well-trained specialized police teams that understand social media is essential.

  In 2018, the Government of Canada announced the creation of a Gender-Based Violence Knowledge Centre at Western University. One of the pillars of this initiative is the "promotion of responsive legal and justice systems."[44] Allocating funding to both policing and building knowledge are key to tackling the greater issue of online harassment and violence.

---

[41] Eckert, S. 2017. Fighting online abuse shouldn't be up to the victims. The Conversation.

[42] Ibid.

[43] State of California Department of Justice. 2016. Attorney General Kamala D. Harris Announces California Cyber Crime Center Initiative in Fresno.

[44] Government of Canada. 2018. Government of Canada launches Gender-Based Violence Knowledge Centre and announces critical research funding.

In 2016, the RCMP conducted a comprehensive review of its handling of sexual assault cases, creating a team to investigate divisional reports, consult with stakeholders and experts, and establish a plan to improve the RCMP's response to these cases.[45] This review resulted in the establishment of a Best Practices Guide for Sexual Assault Investigations, and a training curriculum to better prepare law enforcement. A similar approach should be considered for improving responses to cyber-harassment.

- **Establish, develop and leverage institutional expertise.** U.K.-based Atalanta, an organization dedicated to globally advancing women's political participation, pointed to current efforts by London's Metropolitan Police to establish a Parliamentary Liaison and Investigation Team in order to quickly respond to threats against MPs.[46] This initiative was developed in the aftermath of the murder of British MP Jo Cox. Giving law enforcement the capacity to react to and track all threats made to politicians and candidates enhances opportunity to further safeguard elected officials.
- **Facilitate opportunities for international co-operation.** The borderless nature of the internet, combined with the inconsistent cyber legislation it can produce, presents significant challenges for law enforcement. Examples of successful multi-jurisdictional co-operation between law enforcement on cyber-harassment and abuse are currently limited. Success stories tend to revolve around cybercrimes involving human trafficking, espionage or hacking, child pornography and fraud. For example, in 2013, Europol established a European Cybercrime Centre to strengthen law enforcement's responses to cybercrime and improve co-operation. This initiative resulted in thousands of investigations and hundreds of arrests.[47] A similar model could be considered for cases of cyber-harassment. However, contradictory international interpretations of freedom of expression may serve as a barrier.

Opportunities for Technology Companies

Technology companies are aware of the abuse, harassment and bullying happening on their platforms. Unfortunately, responses to incidents remain inconsistent, lack transparency and aren't well known by the public. Because the marketing and advertising capability of online platforms is exceedingly effective, these companies should:

- **Promote changes being implemented to make platforms safer.** While efforts are being made by companies to make positive product and policy changes, these efforts are often not communicated in an obvious manner to platform users. A Facebook representative interviewed for this report explained the platform primarily communicates its anti-harassment policies and initiatives in two

[45] Royal Canadian Mounted Police. 2016. The way forward: the RCMP's sexual assault review and victim support action plan.

[46] Atalanta. 2018. (Anti)Social Media: The benefits and pitfalls of digital for female politicians, p. 49.

[47] Europol. European Cybercrime Centre: About.

ways: The first is through an online Safety Center, where users can read Facebook's Community Standards and learn about tools and resources available to help facilitate a safe online environment; The second is through partnerships with organizations like Equal Voice and YWCA (in Canada) that are afforded advertising space to promote their initiatives.

In the political space, Equal Voice and Facebook have been co-ordinating efforts both to celebrate women in politics and to educate. For example, #HerVoice: Facebook Safety Tips for Women Leaders was released earlier this year. Technology companies should consider improving and expanding their outreach and communications to ensure their efforts to combat cyber-harassment are clearly conveyed to online users.

- **De-platform harmful users.** Although people with abhorrent views and ideologies have always existed, technology companies have provided an unprecedented opportunity for them to broadcast their messages. "De-platforming" refers to when social media companies remove from their platforms those users who routinely breach their codes of conduct, typically by spreading hate or misinformation. For example, in the past year, infamous conspiracy theorist Alex Jones was de-platformed by most major online platforms, including Facebook, Twitter and YouTube.[48] Social media companies should continue to use this strategy to address the issue of providing problematic users with international platforms to spread hate and misinformation.
- **Understand the pros and cons of anonymity.** Many have pointed to the idea of removing opportunities to engage anonymously on social media as an impactful strategy to reduce harassment. This policy has been implemented in the comments sections of numerous websites including that of the Canadian Broadcasting Corporation. Requiring users to interact using their authentic identities limits their ability to hide behind pseudonyms and has been demonstrated to regulate cyber-harassment behaviour.

  The primary argument against banning anonymity is that members of some marginalized groups (e.g. women, LGBTQ2+, Indigenous)—and specifically those living in countries where freedom of speech is not a protected right—often rely on anonymity as a safeguard against persecution. A 2018 report, funded by Canada's International Development Research Centre, highlighted the importance of anonymity to help "bolster women's ability to express opinions and beliefs and to challenge taboos."[49]

  Another component of anonymity pertains to anonymous reporting. Victims of online harassment are often more likely to come forward when their identity is kept anonymous. Anonymous reporting, however, also has drawbacks. It may be used by harmful actors to drown out legitimate expressions of opinion through targeted campaigns, flagging legitimate content as harassment, and

[48] Hern, A. 2018. Facebook, Apple, YouTube and Spotify ban Infowars' Alex Jones. The Guardian.

[49] Aavriti, N. et al. 2018. Mapping Research in Gender and Digital Technology: Executive Summary. Association of Progressive Communications.

taking advantage of lengthy content-moderation processes by technology companies. Any policy seeking to remove anonymity as a tool for online harassers must balance this risk with the need to safeguard at-risk individuals from persecution for voicing their opinions.

- **Address the legacy of patriarchal culture in technology companies.** It is hard to ignore the "bro culture" of startups and social media companies in general; after all, Facebook (or its predecessor, "Facemash") was a tool developed to rank the appearance of women at Harvard University. This legacy, not unique to Facebook, has manifested in significant gender imbalances in ICT (information and communications technology) and STEM (science, technology, engineering and math) sectors. In Canada, for example, only 26.9% of employees in STEM-intensive occupations are women and only 5% of Canadian technology companies have a solo female CEO.[50] Diverse and inclusionary hiring practices should be company-wide and within all sectors.[51]

In Canada, only 26.9% of employees in STEM-intensive occupations are women and only 5% of Canadian technology companies have a solo female CEO.[52]

Moreover, increased transparency and awareness of the stress factors faced by women working for social media companies—specifically moderators, who often experience mental illness caused by the unpleasant materials they are tasked with observing—will help to improve outcomes for both those experiencing harassment and those tasked with moderating content.

- **Explore opportunities and challenges of using AI.** Efforts to use artificial intelligence to address harmful content online have traditionally focused on combating violent extremism, democratic interference and explicit sexual content. Although in recent years Facebook has been quite successful at proactively flagging and removing this content, it has encountered difficulties developing methods for identifying content that meets the threshold of bullying or harassment—only catching 14.6% through AI and the rest through user reporting. This is because the language of cyber-harassment is contextually and culturally specific, and is often disseminated through coded language, images, gifs, and memes. For this reason, AI is unlikely to fully replace human moderators. It's not a silver bullet to cyber-harassment.

  Beyond using AI as a tool for online moderation, the use of technology to empower and amplify diverse women's voices in politics should be explored. An example of such technology is being tested by Edmonton-based ParityYEG, an organization dedicated to empowering women

[50] #MovetheDial. 2017. Where's the Dial Now: Benchmark Report.

[51] Hempel, J. 2018. How Social Media Became a Pink Collar Job. Wired.

[52] Ibid.

to pursue political office. The organization recently introduced a Twitter bot, ParityBot, designed to respond immediately to harassing, derogatory or misogynistic tweets directed at women running for office. The bot was tested during Alberta's 2019 provincial election, and the volunteer team is preparing for a larger initiative during the 2019 federal election. Although ParityBot presents an interesting example of artificial intelligence used as a force for good, similar initiatives should be implemented with caution to ensure legitimate expressions of opinion are not drowned out by automated counter-messaging.

Enhance Media Standards and Regulation

- **Develop regulatory measures for social media**. Traditional media sources are regulated by strict policies governing conduct, content and transparency. For example, the Canadian Broadcast Standards Council,[53] a national voluntary self-regulatory organization created by Canada's private broadcasters to deal with complaints made by viewers or listeners, has developed policies on everything from depictions of violence, to sexual content, to negative and/or discriminatory portrayals of social groups.[54] Technology platforms, however, are not held to the same standards in Canada. This is partly because these platforms do not neatly fit into categories of telecommunications, broadcasting, or publishing. Governments and relevant stakeholders should consider developing a regulatory framework—whether legally binding or voluntary—establishing rules for appropriate content, transparency, reporting frameworks and moderation practices for social media platforms.

LONG-TERM STEPS: SOCIAL AND CULTURAL CHANGE

Over the past 15 years, online platforms have become the new public square—for better and for worse. These platforms offer their users immediate connections; why write a letter to your local representative, when you can send an email, tweet or Facebook message? Because this phenomenon is still relatively new, society has not fully developed parameters for acceptable, or even legal, behaviour on the internet.

Characteristics of online platforms—namely, anonymity and ease of communication—have allowed hate and harassment to be transmitted in new and unfamiliar ways. Nevertheless, the drivers of this behaviour—

[53] The Canadian Radio-television and Telecommunications Commission (CRTC) requires broadcasters to adhere to the Equitable Portrayal Code, which aims to ensure that media treatment is not discriminatory or biased. Broadcasters are responsible for ensuring their news directors and journalists follow the code. The code was developed by the Canadian Association of Broadcasters, approved by the CRTC, and all broadcasters must adhere to it by condition of licence. Broadcasters and the Canadian Broadcast Standards Council administer the code.

[54] McKelvey, F., Tenove, C. and Tworek, H. 2018. Poisoning Democracy: How Canada Can Address Harmful Speech Online. Public Policy Forum.

specifically, structural and cultural misogyny—have always existed. For this reason, any long-term solution to cyber-harassment will require dramatic cultural and societal transformation.

The following actions have been identified to facilitate a lasting shift in political culture and to make changes to the cultural narratives of who belongs in public life.

- **Development of a standard lexicon**. Terminology pertaining to the online harassment of women has been and continues to be debated. These online behaviours are regularly described as cyberbullying, cyberviolence, and/or cyber-harassment. There is, however, no clear delineation of what each term means or how they are differentiated. This report uses the umbrella term of "cyber-harassment" to describe online behaviours aimed at intimidating, dominating and/or excluding.[55] Many organizations advocate using "gender-based violence" or "technology-facilitated gender-based violence" when referring to harmful online behaviours directed at women.[56]

  Moreover, developing a standard lexicon is further complicated by contradictory interpretations of free speech versus hate speech (both within and across global jurisdictions). For example, the United States' interpretation of free speech is much broader than that of Canada and many other liberal democracies. This poses a problem for international enforcement mechanisms and collaboration.

  Working towards building a standard lexicon for negative online behaviours is important to allow relevant stakeholders to have coherent conversations and facilitate the collection and comparison of data. Even more significant, clear definitions of illegal conduct allow for international co-operation and the development and enforcement of laws and legislation. This outcome will be achieved only through long-term co-operation between a variety of actors, including governments, advocacy organizations, researchers and online platforms.

[55] Council of Europe, Cybercrime Convention Committee. 2018. Mapping study on cyberviolence. This study, conducted by the Council of Europe, outlined the following behaviours as meeting the threshold of cyber-harassment:

1. Unwanted sexually explicit emails or other messages.
2. Offensive advances in social media and other platforms.
3. Threat of physical or sexual violence.
4. Hate speech — meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and/or other traits (such as sexual orientation or disability).
5. Any other online conduct aimed to harm (e.g. cyberbullying, doxing, revenge porn).

[56] Hinson, L., et al. 2018. Technology-facilitated gender-based violence: What is it, and how do we measure it? International Center for Research on Women. The centre describes technology-facilitated GBV as: "action by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms. This action is carried out using the internet and/or mobile technology and includes stalking, bullying, sexual harassment, defamation, hate speech and exploitation."

- **Better data collection**. In its Elect Her report, FEWO issued a recommendation for the Government of Canada to increase funding to Statistics Canada so that it could expand survey data collection on the participation and engagement of diverse groups of women in political activities.[57] This collection would go beyond women's political leadership. It would also include their engagement in other facets of political life, for example volunteering and donating to a political party. Data collection should also be expanded to include incidences of harassment of women in politics, to gauge the prevalence and characteristics of harassment and its impacts—and in turn, shape policies and legislation.

- **Broader education initiatives on gender equality and digital citizenship.** Further recommendations in FEWO's report aimed to improve education initiatives on gender equality. One recommendations called for the federal government to implement an education initiative, with the goal of shifting how women in politics are perceived.[58] This recommendation is rooted in overwhelming evidence that the conduct of women in politics is perceived and reacted to in vastly different ways than their male counterparts.[59] The report further called for provincial and territorial ministers "responsible for Education… to encourage all jurisdictions to incorporate the topics of gender equality, gender stereotypes and women's participation in politics into their education curricula."[60] Breaking down long-standing stereotypes about women—through campaigns, school curricula, and GBA+[61]—will help change the often toxic culture in which women in politics operate.

  Another education initiative that could address the problem of cyber-harassment of women in politics is improved digital literacy and citizenship training. The Government of Canada, with the support of organizations active in this space, should co-ordinate initiatives to ensure Canadians know how to operate safely and responsibly in online environments.

[57] Standing Committee on the Status of Women. 2019. Elect Her: A Roadmap for Improving the Representation of Women in Canadian Politics.

[58] Ibid.

[59] Daughters of the Vote. 2019. 77% of Canadians believe men and women are treated differently in politics, according to new national poll. Equal Voice.

[60] Standing Committee on the Status of Women. 2019. Elect Her: A Roadmap for Improving the Representation of Women in Canadian Politics.

[61] GBA+ is an analytical process used to assess how diverse groups of women, men and non-binary people may experience policies, programs and initiatives. The Government of Canada recently renewed its commitment to GBA+ and is working to strengthen its implementation across all federal departments.

CONCLUSION

There is no silver bullet solution to the cyber-harassment of women in politics and no single institution or organization that can unilaterally solve the issue. A collaborative approach to creating an environment where women are not only safe but empowered to voice their political opinions will require a multi-dimensional framework of short-term, medium-term, and long-term actionable steps by actors both within and outside government.

Short-term Steps

Over the short term:

- political parties should take a leadership role by training all campaign team members on codes of conduct and anti-harassment policies; and
- government and civil society should support organizations whose goal is to increase women's participation in politics, including ones providing digital resilience and bystander training.

Medium-term Steps

Medium-term considerations need to include the implementation of stronger laws and standards to address and deter the cyber-harassment of women, including:

- improving law enforcement through consistent cyber-related legislation, training and resource allocation, and opportunities to leverage and develop institutional expertise; and
- assisting and giving incentives to technology companies to implement changes to their platforms and adopt standards that prevent cyber-harassment online.

Long-term Steps

The internet is a relatively new phenomenon. Misogyny and violent harassment, however, are not. While society tries to catch up to the changes brought about by the Internet—specifically its ability to facilitate and amplify harmful behaviour—real and lasting change will be seen only through social and cultural shifts occurring over the long term. Long-term change requires:

- agreed-upon language regarding online harassment and violence in order to tackle it through law enforcement;
- improvements in data collection to better understand the nature and extent of the problem; and
- a focus on education of gender equality to shift attitudes towards women in politics.

During a March 12, 2019, address to the United Nations' 63rd session of the Commission on the Status of Women, UN Secretary General António Guterres stated:

> **"When we exclude women, everyone pays the price. When we include women, the whole world wins."[62]**

Hearing from diverse voices is good for political discourse. Diversity in Canadian politics yields new and innovative ideas, policy solutions and ways of doing things. Encouraging women to participate in political life is good for democracy. The women who choose to run for political office sit on either side of the political spectrum, often advocating for divergent and competing issues. Cyber-harassment of women in politics is therefore not a partisan or a gendered issue. It is everyone's problem and, in turn, everyone's responsibility to solve.

[62] Guterres, A. 2019. Remarks at the opening of the 63rd session of the Commission on the Status of Women. United Nations

APPENDIX

Solutions to Cyber-Harassment Aimed at Women in Political Life

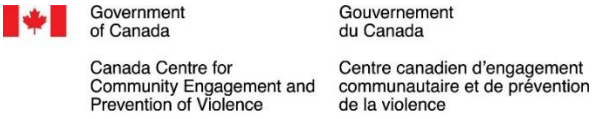
Tuesday, Feb. 19, 2019 | 8 a.m. to 12 p.m.
Fairmont Château Laurier (1 Rideau Street, Ottawa) | Renaissance Room (Mezzanine Floor)

AGENDA

8:00 a.m.	**Registration and Breakfast** Hot breakfast will be available
8:30 a.m.	**Welcome and Introductions** **Julie Cafley**, Executive Vice-President, Programs & Partnerships, Public Policy Forum **Johanne Senécal**, Senior Vice-President, Government Relations and Regulatory Affairs, TELUS
8:40 a.m.	**Keynotes** **Michele Austin**, Head of Government, Public Policy and Philanthropy, Twitter Canada **Nancy Peckford**, Mayor of North Grenville and Executive Director of Equal Voice
9:00 a.m.	**PANEL—How do We Solve Cyber-Harassment Affecting Women in Public Life?** **Panelists:** **Seyi Akiwowo**, Founder and Executive Director, Glitch **Kathy Macdonald**, Presenter, instructor and cyber awareness specialist, and former police officer **Sandra Pepera**, Director of Gender, Women and Democracy, National Democratic Institute **Chris Tenove**, Postdoctoral Fellow in Political Science, University of British Columbia **Moderator: Vassy Kapelos**, Broadcast journalist, host of Power & Politics, CBC
10:15 a.m.	**Break**
10:30 a.m.	**Roundtable Conversation** **Moderator: Vassy Kapelos**, Broadcast journalist, host of Power & Politics, CBC
11:45 a.m.	**Closing Remarks** **Danielle Takacs**, Manager, Federal Government Relations, TD Bank Group

Thank you to our partners:














PUBLIC
POLICY
FORUM