

Spring 2022

Technological Threats: How Online Harassment of Female Political Figures Undermines Democracy

Madeleine Songy, Madeleine Pelton, Olivia
Cretella, Areala Mendoza, Kathryn Hopp, Olivia
Jackson, and Ailyah Banks

FACULTY ADVISOR

Dr. Valerie M. Hudson

The Bush School
OF GOVERNMENT & PUBLIC SERVICE
TEXAS A&M UNIVERSITY 

Table of Contents

Executive Summary.....	3
Scope/Defining our Target Population.....	4
Thank You to Our Experts.....	5
<i>Table 1. List of Experts</i>	6
Explaining Current Definitions.....	7
<i>Online Harassment, Online Abuse, and Technology-Facilitated Gender-Based Violence</i> ..	7
<i>Gendered Disinformation</i>	8
<i>Online Environment</i>	9
<i>Table 2. Characterizing the Online Environment</i>	10
<i>Table 3. Key Technologies</i>	9
<i>Table 4. Types of Social Media Networks</i>	10
<i>Victims</i>	12
<i>Perpetrators</i>	12
<i>Democratic Backsliding</i>	13
Why Threats to Women’s Political Participation are Threats to Democracy.....	14
<i>Table 5. Indicators of Authoritarian Behavior that Reinforce Digital Misogyny and Contribute to Democratic Backsliding</i>	14
How Prevalent is Gender-Based Online Harassment?	16
<i>How online harassment has changed over time</i>	16
<i>Escalation to Physical Violence</i>	18
<i>A Multinational Pandemic</i>	20
<i>Figure 1. A Map of Countries Examined in A Multinational Pandemic</i>	28
Effects of Gender-Based Online Harassment on Women’s Political Participation.....	27
<i>Intersectionality Matters</i>	27
<i>Levying Heavy Costs on Political Engagement</i>	29
<i>The More Women, the Greater the Outrage</i>	31
<i>Effects on Democracy</i>	31
Existing Policies and Programs.....	33
<i>Major Trends in Regional and Country Responses to Online Harassment</i>	34
<i>Figure 2. Map of Summit for Democracy Countries that made policy commitments involving technology and/or women’s rights</i>	35
<i>Enhancing Legislation on Gender Discrimination in Latin America</i>	41
<i>Data Protection and Online Safety Initiatives in Europe</i>	42
<i>Non-State Actors and NGOs Respond to Online Harassment</i>	44
<i>Barriers to Policy Responses: MENA and Why WhatsApp?</i>	47
Gaps in the Research and Literature.....	48
Policy Recommendations.....	50

Conclusion.....	67
Bibliography.....	68
Endnotes.....	78

Executive Summary

The rapidly evolving technological landscape presents unprecedented opportunities and challenges for national and international communities. These challenges increasingly concern the technology-facilitated harassment and abuse perpetrated against women and minority groups, a phenomenon that occurs on social media platforms and through the abundance of communication technologies available to most individuals. Women across the globe who choose to participate in political life, and especially those who choose to serve in leadership positions, must simultaneously come to terms with the inevitable harassment that awaits them in the digital sphere.

Amid growing concerns over the vitality and sustainability of democracy and the value of democratic principles, attacks on female political actors in democratic spaces cannot be ignored. In addition to direct attacks, gendered disinformation, a tactic employed particularly against elected and appointed politicians to undermine women’s credibility and influence public opinion, finds sturdy foundations in the online environment. Gendered disinformation’s partnership with technologically-facilitated methods of communication exacerbates the already challenging environment in which female politicians operate and heightens the range of political, social, and emotional effects they experience. These online gender-based attacks give way to potential escalation to violence against women and further challenge the full and active participation of all women in political spaces. When half of a national community is unable to effectively and successfully participate in the democratic process, democracy fails.

This report outlines the current research landscape that falls at the intersection of online harassment, technology, and women’s political participation. Looking through the lens of female political figures allows for an understanding of the obstacles that confront women’s political participation within leadership, arguably one of the highest levels of democratic participation. First, the background of this report explains and synthesizes current definitions relevant to this topic. Second, it draws the connection between democracy and women’s political participation,

emphasizing the phenomenon that is democratic backsliding. Third, this report discusses the evolution of this issue over time and the prevalence of online harassment across the international environment. Fourth, the effects of technology-facilitated online harassment are discussed, emphasizing the differences in experiences of women with varying intersectional identities. Fifth, the report maps existing policies and programs, national legislation and policy recommendations, as well as surveying the gaps in literature observed from that exercise. The report concludes with a comprehensive discussion of policy recommendations for U.S. government agencies, U.S. legislation, and the private sector.

Scope/Defining our Target Population

Women who step into online spaces face a slew of hostilities, falling victim to objectification, scrutiny, harassment, and even violence. This report examines the phenomenon of online harassment as it pertains to women's political participation, specifically deconstructing the online harassment of elected and appointed female political figures. Through the investigation of this subsection of gender-based online harassment, this paper contributes to the understanding of the adverse relationship between online harassment and women's political participation. We survey literature which focuses on the online harassment of current or former female political figures who were either elected or appointed, as well as women who are or were running for office. For the present effort, the focus of the literature review is on female politicians, and not political activists, journalists, reporters, and voters, though we believe that would be a fruitful line of inquiry for those interested in democratic trends. In addition to the experience of politicians, we are also interested in governmental and societal responses to this problem. We review actions taken by countries, NGOs, private entities, and multilateral organizations to address the problem. Due to timing and resources, the scope is also limited to English-speakers in interviews and English-language source materials. However, English-language documents available from non-English speaking countries were reviewed to analyze current national initiatives. Despite these delimitations, we believe the overall parameters of the problem can be broadly sketched, and best practices of public and private response identified.

Thank You to Our Experts

Through the course of this research, our team had the opportunity to interview several renowned researchers who work within this space and whose time and insight substantially impacted the direction of our research: Saskia Brechenmacher, Julie Denham, Caroline Hubbard, Lucina Di Meco, Dr. Josefina Erikson, Dr. Cecilia Josefsson, Nina Jankowicz, Dr. Jocelyn Kelly, Min Kyriannis, and Dr. Sarah Sobieraj. The expertise of these ten professionals spans the breadth of this issue, specializing as they do in democracy, women, peace, and security, governance, and gender issues falling within private, government, and academic spaces.

Our conversations with these experts contributed to our understanding of terminology, current environment, and policy approaches. Each interview contributed immeasurably to the contextualization of this issue within the global context of democracy. Through conversations with Dr. Erikson and Dr. Josefsson, we were able to develop an introductory understanding of how other democracies deal with and approach this issue. Saskia Brechenmacher emphasized the importance of intersectionality when discussing the consequences of gender-based online harassment and the disproportionate impacts on women whose identities differ across social, cultural, economic, ethnic, and political backgrounds. Julie Denham and Caroline Hubbard introduced the connection between online harassment and gender-based violence, contributing to the construction of our mapping of current country policies that prioritize technology and gender and those that have attempted to legislate on this particular issue. Lucina Di Meco and Nina Jankowicz emphasized the importance of understanding gendered disinformation, considering this phenomenon grants a holistic understanding of the online and offline impacts that female political figures experience. Dr. Jocelyn Kelly reinforced our arguments on this issue's impact on democracy by orienting our research towards tangible datasets concerning indexes on violence against women, democracy, and women's political participation. Min Kyriannis gave acute insight into the relationship between the tech sector and the U.S. government as well as recommendations for best practices on public-private engagement. Dr. Sarah Sobieraj assisted us in compiling a list of critical gaps in research and available data.

Table 1 displays the name, title, and entities associated with each interviewee and summarizes the main points covered in each interview.

Table 1. List of Experts

Name	Position	Entities	Key Topics Discussed
Saskia Brechenmacher	Fellow, Democracy Conflict & Governance	Carnegie Endowment for International Peace	Intersectionality, Democratic Backsliding, Examining Non-Western Democracies
Julie Denham	Senior Advisor, Elections and Political Transitions	USAID	Technology-Facilitated Gender-Based Violence, Latin America and Caribbean GBV Laws, Connection between Democracy, Human Rights, and GBV, Online Harassment as a Continuum
Caroline Hubbard	Senior Gender Advisor		
Lucina Di Meco	Co-Founder	#ShePersisted	Gendered Disinformation, Connection to Disinformation/Misinformation More Broadly, Standardization of Guiding Principles/Code of Conduct, Encourage Funding
Dr. Josefina Erikson Dr. Cecilia Joseffson	Associate Professors	Uppsala University, Sweden	Specifics on Women in Swedish Parliament and Policy Recommendations for Internal Legislative Practices, Perspective on Differences in Western Democracies
Nina Jankowicz	Senior Adviser <i>Author, How to be a Woman Online</i>	Centre for Information Resilience The Wilson Center	Use of “Online Harassment”, Impacts on Democracy and Women, Gendered Disinformation, Current International Framework Laws, and Applicability to Online Harassment
Dr. Jocelyn Kelly	Director, Program on Gender, Rights, and Resilience	Harvard Humanitarian Initiative	Democracy and Social Cohesion, Fragile States, and Statistical/Data-Backed Support
Min Kyriannis	CEO & Founder Co-Founder	Amyra Systems Inc. GlobalCyberConsortium	Private Sector Engagement on the Policy Front, Recommendations for Technology Companies, Preventing Cosmetic and Superficial Measures
Dr. Sarah Sobieraj	Professor, Sociology <i>Author, Credible Threat</i>	Tufts University, Maryland	Outline Research Gaps, Programs Oriented Around Victim Services, Push for More Funding on Research Areas

Explaining Current Definitions

Online Harassment, Online Abuse, and Technology-Facilitated Gender-Based Violence

Relevant literature uses various terms to describe the phenomenon of online attacks against women, beginning with online harassment and further defining escalations under online abuse and technology-facilitated gender-based violence to assess severity. A general interpretation of the following three terms, which are used somewhat interchangeably across the surveyed literature, yields the conclusion that harassment differs from abuse in that the latter promotes violence. Meanwhile, the difference between online abuse and technology-facilitated gender-based violence (TFGBV) is somewhat negligible. The use of TFGBV is found in more recent reports on the issue and seems to have been applied for rhetorical effect rather than to characterize a shift in method or consequences.

Online harassment is defined as “offensive name-calling online, intentional efforts to embarrass someone, physical threats, stalking, sexual harassment, or harassment over a sustained period of time.”¹ Online harassment is an ongoing behavior rather than an isolated incident that uses technology to repeatedly “contact, annoy, threaten or scare another person.”² When online harassment is perpetrated on the basis of the survivor’s gender, sexuality, or sexual orientation it constitutes a form of Technology-Facilitated Gender-Based Violence.³ In *Credible Threat: Attacks Against Women Online and the Future of Democracy*, Sarah Sobieraj characterizes online harassment against women as expressions of “digital misogyny” and “patterned resistance” against women’s full and equal participation in public life. She argues that the attacks are “aimed at protecting and reinforcing a gender system in which women exist primarily as bodies for male evaluation and pleasure.”⁴ Online harassment can take the form of sexist, racist, transphobic, or other offensive language that concerns itself with a woman's identity. Harassment does not inherently promote offline violence, but it is persistent and patterned and has the goal of overwhelming or distressing its target.

Online abuse takes harassment a step further in that it “promote[s] violence against or threaten[s] people based on their race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease. Online abuse is a digital manifestation of identity-based attacks⁵ and ‘is a problem that all politicians confront’”⁶ It can be thought of as the technological side of social prejudice, demonstrated by online expressions of

racism, sexism, xenophobia, and homophobia. Examples include physical or sexual threats, wishes for physical harm or death, reference to violent events, behavior that incites fear or repeated slurs, epithets, racist and sexist tropes, or other content that degrades someone”.⁷ The distinction between online harassment and online abuse concerns the likelihood of escalation to violence. Online abuse is the “most common type of psychological abuse experienced by women in politics” that increases in severity for women who are “member[s] of one or multiple marginalized groups, speaking up about feminist issues or those that otherwise challenge the status quo, and [are] speaking in a male-dominated space”.⁸

Technology-facilitated gender-based violence is the most recent attempt at a terminology to use in describing the online abuse of women. Technology-facilitated GBV is perpetrated by any type of “communication technologies, such as cell phones, email, social networking sites, chat rooms or online dating sites and apps to commit or procure sexual assault or abuse”.⁹ TFGBV is part of the continuum “of multiple, recurring and interrelated forms of gender-based violence against women and girls” that occur throughout a woman’s life.¹⁰ TFGBV is “rooted in, driven by, replicates and reinforces the same structural gender inequalities and sexist and misogynistic beliefs, norms and institutions that underpin other forms of GBV.”¹¹

Gendered Disinformation

Disinformation is the deliberate and covert spreading of false information to influence public opinion or obscure the truth. Gendered disinformation is one form of online disinformation and is defined as “a subset of online gendered abuse that uses false or misleading gender and sex-based narratives against women, often with some degree of coordination, aimed at deterring women from participating in the public sphere.”¹² Gendered disinformation creates a narrative surrounding a woman that associates her with a social stigma, often for some type of proscribed sexual behavior outside of society’s norm. The report *Malign Creativity* analyzed messages on various social media platforms and found that disinformation campaigns against women in politics typically fell under three categories; transphobic narratives, racist narratives, and sexualized narratives.¹³ A woman can be delegitimized as a political leader by the way she dresses, her sexual past, her race, sexual orientation, religion, or her current relationship status. For example, Representative Ilhan Omar of Minnesota has been the target of disinformation

campaigns targeting her identity as a Black and Muslim woman. Disinformation narratives identified in the data collected in *Malign Creativity* portray Omar as a “terrorist and political saboteur;” claims based on her identity as a refugee in both the Black and Muslim community.¹⁴ In Kenya, disinformation campaigns often target a woman’s marital status, claiming singleness as a negative factor tainting her ability to lead politically. Another popular avenue of gendered disinformation is claiming that a woman is unfit to hold positions of power based on her perceived promiscuity. For example, during the 2020 Presidential campaign, Kamala Harris was targeted by gendered disinformation campaigns concerning her sexual past in an attempt to discredit or humiliate her, a common objective for many perpetrators of online harassment.¹⁵ Vice President Harris’s sexual past, like other female political figures, became a fundamental target for online abusers in their campaigns of social stigmatization. Rumors spread about women’s characters as ‘homewreckers’ who employ sex to achieve their career goals, despite circumstances demonstrating the opposite. For Vice President Harris, this narrative that she uses sex to advance her career directly targets her perceived legitimacy to hold office.¹⁶ Gendered disinformation campaigns don’t just affect the woman they are targeting; they affect all women who seek to participate in the public sphere. Disinformation campaigns are popular political strategies for authoritarian forces that have the broader goal of delegitimizing *all* women from political participation by painting a picture of women as “devious, stupid, overly sexual or immoral and therefore, unfit for public life.”¹⁷ Disinformation campaigns are dangerous for democracy, whether they target men or women, but the increase of sexualized and gendered disinformation serves to delegitimize women’s rights to political leadership and threatens women’s political participation.

Online Environment

The **online environment** consists of digital technologies created by private tech companies. Digital technologies consist of “electronic tools, systems, devices and resources that generate, store or process data... includ[ing] the infrastructure, devices, media, online services and platforms that we use for communication, information, documentation, networking,...relationships,...and identity needs.”¹⁸ They include, but are not limited to: designated internet service providers, social media service providers, electronic service providers, app distribution service providers, hosting service providers, hardware development companies, and software development companies.¹⁹ See Table 2 below for examples of each.

Table 2. Characterizing the Online Environment.

Private Technology Company Type	Examples
Designated Internet Service Providers <i>Access online materials</i>	Google, Safari, Internet Explorer, Firefox
Social Media Service Providers <i>Two “end” users online</i>	Twitter, Facebook, LinkedIn, Instagram, TikTok, Snapchat
Electronic Service Providers <i>“End” user communication</i>	Outlook, Twitch, Discord, Slack
App Distribution Service Providers <i>Access to app services</i>	Google Playstore, IOS App Store
Hosting Service Providers <i>Hosting or stored materials</i>	Apple iCloud, Google Drive, Microsoft Office 365 (SharePoint), Amazon Web Services
Hardware Development Companies <i>Create, develop, and/or maintain</i>	Technology Equipment and Physical Assets (i.e., laptops, smartphones, hard drives, etc.)
Software Development Companies <i>Create, design, develop, and maintain programs</i>	Microsoft, Cisco, Adobe, Intel, GitHub, Stack Overflow, SAP

Tables 3 and 4 outline key terms necessary for understanding gender-based online harassment. Table 3 outlines various programming mechanisms that may help or hinder online harassment and abuse and provides a solid definition for **social media**. Table 4 outlines the various types of social media platforms and examples of each.

Table 3. Key Technologies.

Key Technologies	Definition and Examples
Algorithm	“An algorithm is a procedure or formula for solving a problem, that is, a series of

	instructions that tell a computer how to transform a data set into useful information. Algorithms are widely used throughout all areas of information technology.” ²⁰
Artificial Intelligence	“Artificial intelligence is a field that combines computer science and robust data sets, to enable problem-solving. It also encompasses subfields of machine learning and deep learning, which are frequently mentioned in conjunction with artificial intelligence. AI seeks to create expert systems which make predictions or classifications based on input data and leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind.” ²¹
Bots	Shorthand for “software robots,” typically automated in some fashion, either fully automated or human-in-the-loop. Can consist of spam or malware, be benign, or used for social good. Can function in coordination with one another becoming “botnets.” ²²
Social Media	“Social media is a collective term for websites and applications that focus on Internet-based communication, community-based input, interaction, content-sharing, and collaboration. Forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media that allow quick electronic communication of content to users.” ²³

Table 4. Types of Social Media Networks.

Types of Social Media Networks	Examples
Social Networks	Facebook, Twitter, LinkedIn, WhatsApp
Media Sharing Networks	Instagram, Snapchat, Youtube, Tiktok, VSCO

Discussion Forums	Reddit, Quora, Digg
Bookmarking and Content Curation	Pinterest, Flipboard
Consumer Review Networks	Yelp, Zomato, TripAdvisor
Blogging and Publishing	WordPress, Tumblr, Medium
Social Shopping Networks	Polyvore, Etsy, Fancy, Poshmark, Depop, Mercari

Victims

Though women and girls of all ages can be victims of online harassment and abuse, there are specific groups that experience higher than normal levels. These groups include adolescent girls, women in public and professional life, and women with intersecting identity factors.²⁴ The term **victim**, as described in this report, is primarily associated with women in public and professional life. The particular focus on this group of women is due to the fact that women in public and professional life are “disproportionately targeted...when their professional lives are supported by an online presence...[that] engag[es] with the broader public,” when they “use digital platforms for activism and issue-based advocacy,”²⁵ and if they “achieve high leadership positions.”²⁶ The types of issue-based advocacy that tend to garner the most backlash concern are, broadly, “political issues, feminism, race or sexual and reproductive health and rights.”²⁷

Perpetrators

Just as online harassment is facilitated through various forms, it is perpetrated by various types of people. In the United Nations Population Fund’s 2021 report on technology-facilitated gender-based violence, they characterized the different types of **perpetrators** of TFGBV. Online harassment can come from friends, colleagues, and total strangers.²⁸ Recently, the rise of social media created a space for more anonymous and collective group attacks toward women.²⁹ For the average woman, TFGBV is most likely to stem from a current or former intimate partner.³⁰ However, the main perpetrators of harassment change when considering women political figures. State actors are the primary perpetrators of TFGBV towards women engaging in politics.³¹

Leading state actors that have the technology and authority threshold to control the messages fellow citizens receive may use their power to diminish the voices of women political actors.³² Following state actors, anonymous individuals and political opponents are the next most likely source. It should also be noted that online harassment does not solely stem from anonymous individuals or political opponents; it can even come from one's own political party. Party affiliation does not protect women from online threats. Online harassment is perpetrated from every avenue; there is no safe area on the internet for female political figures.

Democratic Backsliding

Democratic backsliding is the gradual erosion of democratic norms over time in a country. It is the movement of liberal democracy towards an illiberal or authoritarian regime. Authors Steven Levitsky and Daniel Ziblatt discuss how democratic backsliding can be observed and measured when political leaders abandon a foundational norm of democracy: mutual toleration.³³ Mutual toleration is the “understanding that competing parties accept one another as legitimate rivals.”³⁴ The phenomenon of online harassment against women, when perpetrated by or encouraged by politicians, violates the norm of mutual toleration. When women in politics are constantly harassed, abused, and are targets of disinformation campaigns online, the goal is to deny their legitimacy to participate in public life.³⁵ Levitsky and Ziblatt argue that democratic backsliding via the violation of mutual tolerance can look like leaders claiming that their rivals are threats to the nation's security or to the nation's “way of life,” that their rivals are criminals, or that their rivals are “foreign agents” working for an enemy government.³⁶

As mentioned previously in the definition of gendered disinformation, many of the false narratives spread about female politicians can be understood through the lens of anti-democratic conduct by seeking to deny the legitimacy of political opponents. Another form of this behavior that lines up with democratic backsliding and online abuse of women is toleration or encouragement of violence.³⁷ The lack of political will to stop or prevent the abuse of women online, and in some cases, the perpetuation of such abuse by state actors, are symptoms of a larger phenomenon of the erosion of democratic norms.

Table 5. Indicators of Authoritarian Behavior that Reinforce Digital Misogyny and Contribute to Democratic Backsliding.

Denial of the legitimacy of political opponents	Toleration or encouragement of violence
Do they describe their rivals as subversive, or opposed to the existing constitutional order?	Do they have any ties to armed gangs, paramilitary forces, militias, guerrillas, or other organizations that engage in illicit violence?
Do they claim that their rivals constitute an existential threat, either to national security or to the prevailing way of life?	Have they or their partisan allies sponsored or encouraged mob attacks on opponents?
Do they describe their partisan rivals as criminals, whose supposed violation of the law (or potential to do so) disqualifies them from full participation in the political arena?	Have they tacitly endorsed violence by their supporters by refusing to unambiguously condemn and punish it?
Do they suggest that their rivals are foreign agents, in that they are secretly working in alliance with a foreign government, usually an enemy one?	Have they praised (or refused to condemn) other significant acts of political violence, either in the past or elsewhere in the world?

Source: Levitsky, S. & Ziblatt, D. (2019) How Democracies Die. Broadway Books.

Why Threats to Women's Political Participation are Threats to Democracy

Democracies provide their citizens with certain fundamental rights and freedoms, such as freedom of speech, freedom of worship, etc, and at the minimum provide their population with the right to express their political ideas and opinions through voting in free and fair elections.³⁸

Women's equal access to political spaces is an important aspect of democracy which is threatened by online abuse against women. Hillary Clinton once said that "There cannot be true democracy unless women's voices are heard. There cannot be true democracy unless women are given the opportunity to take responsibility for their own lives."³⁹ According to Clinton, a good indicator of political reform is how governments treat their women.⁴⁰ The health of a democracy may therefore be gauged by the opportunity and treatment afforded to women who engage in the political process. Political scientists agree that women's civil rights are an integral part of democracy, but they are only recently coming to the understanding that women's civil rights are a necessary precondition for democracy.⁴¹ Patriarchal authoritarian regimes, therefore, have good

reason to push back against women's political participation: "when women participate in mass movements, those movements are both more likely to succeed and more likely to lead to more egalitarian democracy."⁴² Women make up almost 50% of the world's population, and more than 50% in most liberal democracies. In a healthy democracy, their opportunities should reflect their share of the population. The right of political participation for all peoples, regardless of sex, gender, race, etc, is vital for a healthy democracy. When this democratic principle is undermined via online harassment, abuse, and threatening of women in public spheres, democracy is in danger.

Even if an individual woman is not directly targeted by online harassment, the abuse affects her online participation.⁴³ Those directly targeted often withdraw from online engagement, platforms, and services, but it is also true that other women and girls who witness gendered online harassment are likely to "modify their online behavior, restricting and censoring what they post online, and withdrawing from digital spaces and services due to concerns they too will be targeted with threats, intimidation, stalking and abuse online."⁴⁴

As a result of online abuse against women and their subsequent self-censorship, there is a systemic impact that enforces "patriarchal gender roles, discourages women from taking up leadership roles, and reduces online content related to equality and human rights."⁴⁵ Besides presenting obstacles to women's political involvement, online abuse against women in politics is a fundamental violation of women's human rights, including "rights to health and bodily integrity, rights to live free from violence, rights to freedom of expression and access to information, and rights to privacy and data protection."⁴⁶ Online abuse against women is a form of discrimination against women and a human rights violation falling under the UN Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW).⁴⁷ Violence and harassment perpetrated against women in politics are increasingly recognized around the world as barriers to women's political participation.⁴⁸

Online harassment may seem like a trivial matter to those who have not experienced it, but it is a serious symptom of a more malignant disease that is eroding democracy around the world. When online harassers threaten women in politics with rape or other violence, criticize their appearance, attack their identities, or spread harmful rumors about their private life, the goal (as well as the effect) is to silence women and uphold the patriarchal status quo which is authoritarian by nature.⁴⁹ The pushback of women's rights via online abuse thus accompanies a

broad assault on democracy. According to Freedom House and the Varieties of Democracy Project, the last 15 years have seen democratic backsliding and rising authoritarianism worldwide: it is not a coincidence that women's equality is being rolled back at the same time that authoritarianism is on the rise.⁵⁰ Politically active women are a threat to authoritarian (and aspiring authoritarian) leaders who may rest their claims to legitimacy on patriarchal foundations. This threat of women in politics to autocrats provides a contextual background for the online abuse of women as a political strategy.

How Prevalent is Gender-Based Online Harassment?

How online harassment has changed over time

As technology has evolved, online harassment has proliferated. With the emergence of the Internet, chat rooms soon followed in the late 1990s, such as AOL Instant Messenger.⁵¹ These online forums allowed users to have one-on-one conversations, communicate in public chat rooms, and create group-specific chat rooms.⁵² With the help of digital network phones and personalized computers in the 1990s, chat rooms became a communal breeding ground for users to connect, communicate, and ultimately abuse each other.⁵³ Further progress on the internet increased demand for more sophisticated forms of communication and interaction, thus the introduction of social media. In August 2003, MySpace, the pioneer of social media, launched its social networking service allowing individual users to create their unique profiles and interact in cyberspace with friends and foes alike.⁵⁴ In 2004, came the emergence of Facebook and Twitter followed in 2006. The author asserts that the surge of social media platforms has created increased vulnerabilities amongst internet users.⁵⁵ Users are more vulnerable to the online publication of private information and images along with being harassed by alias profiles.⁵⁶ The ability for users to hide behind alias profiles provides them with an opportunity to say and do anything to another individual.⁵⁷ This presents a perfect opportunity for users to contribute to online abusive language, threats of rape, doxing, deep fakes, and sharing images without consent or the worry of repercussions.

Over time, there has been a gradual increase in sophistication from low-tech mechanisms to conduct online harassment to more advanced forms of technology. This allows for greater ease of access to personal information to facilitate harassment. In an increasingly technological world,

the gradual digitalization of all aspects of life has allowed for the creation of “a virtual world without boundaries where identities can be changed and anonymity is commonplace” and as a result, “women’s risk for experiencing harassment online may be greater than in the “real” world.”⁵⁸ Scholars have also pointed to the involvement of broadband in advancing technology as a critical factor to the facilitation of online abuse due to it enabling the exchange of video, photos, and audio.⁵⁹ This enhanced communication technology has allowed perpetrators of harassment to share digital media for malicious intent with ease.

The growing dependence on digital technology and online platforms often reinforces a sense of an anonymous and lurking threat.⁶⁰ Since the advent of affordable personalized computers, the weaponization of technology-facilitated harassment has increased in scale, from being experienced by only a few women online via only a few channels, to being experienced by many women via multiple platforms.⁶¹ In 2015, the UN Broadband Commission reported that 73 percent of women and girls have been exposed to or experienced some form of online abuse, with women being 27 times more likely to experience online abuse than men and 61 percent of online harassers being male.⁶² Online spaces appear to have developed into a fraternity-like culture that aims to target and exclude women.

Early instances of harassment found on online message boards in the late 1990s contained harsh judgments on women’s physical appearance or sexual attractiveness, focusing not just on their ‘fuckability’ but their ‘rapeability.’ Other findings included abusive language, hyperbolic misogyny, homophobia, and prescribed coerced sex acts as all-purpose correctives. Author and journalist Emma Jane shared the type of messages she regularly received in 1998 after adding her email address to her articles. Jane explains that emails and messages with abusive rhetoric were not rare during this time period: online harassment was relatively contained and not very visible because, generally, only the target would be reading the attacks, and the harassment could be considered spur-of-the-moment individual reactions.

With the advent of social media platforms like Facebook and Twitter, online harassment has shifted into being “viral, quasi-coordinated, and eminently visible.”⁶³ The National Democratic Institute’s study on violence against women in politics discovered that recent advancements in technology expanded the range of perpetrators to include anonymous actors working on their own or as part of large online mobs⁶⁴. These actors intimidate and publicly humiliate women active in the public sphere.⁶⁵ The author uses the case of Kathy Sierra, a

leading figure in the tech industry, to present this shift in online harassment. The cyberhate attack on Kathy Sierra was one of the first to make international media headlines.⁶⁶ In March 2007, Sierra made online remarks on how she didn't moderate comments on her blog, but she respected those who did.⁶⁷ Her antagonists viewed her comment as an unacceptable assault on the liberty of the internet and called for the masses to send her offensive material.⁶⁸ As a result, Sierra received hundreds of rape and death threats from anonymous bloggers and had her social security number and address leaked online.⁶⁹ To protect herself, Sierra began withdrawing from speaking engagements, stopped writing for her blog, and she removed herself from public spaces for years.⁷⁰

In addition to Sierra's experience, there is the case of Anita Sarkeesian whose ongoing activism against sexist tropes in video games has rendered her 'hate-worthy' since 2012.⁷¹ Sarkeesian was the victim of image-based harassment including pornographic photo manipulations and 'rape drawings' of her being "sexually assaulted by the Nintendo video game character Mario."⁷² A video game even surfaced online titled "Beat up Anita Sarkeesian" where players were invited to "punch this bitch in the face."⁷³ The experiences of women such as Sierra and Sarkeesian are evidence not only of the level of risk women face in online spaces, but how online harassment against women has become organized, violent, and more public.

Escalation to Physical Violence

Online harassment can escalate into physical violence. While the escalation to physical violence is less common as compared to online harassment, online abuse, and intimidation, it is still problematic.⁷⁴ The Armed Conflict Location & Event Data Project's (ACLED) report *Violence Targeting Women in Politics: Trends in Targets, Types, and Perpetrators of Political Violence* demonstrates an increase in physical violence directed towards women in politics since roughly 2015.⁷⁵ Globally, political scientists Krook and Restrepo Sanin find that almost all female members of parliament (MPs) have faced psychological violence, and about one-fourth have experienced some sort of physical violence.⁷⁶ A Mexican female political candidate was shot and killed by men in 2018, a chairwoman in Manila was killed in a vigilante-style attack in 2019, and a councilwoman in Moldova was severely beaten in 2020.⁷⁷ In countries like New Zealand and the United Kingdom, the level of physical violence is also high. Polls of New

Zealand and British female politicians show that 80% to 90% of these women experienced aggressive behavior, in the form of a physical attack, stalking and threats in person, or property damage.⁷⁸

Some shocking instances include the case of Mexican political candidate Guadalupe Avila Salinas who was shot during a meeting for women in the community in 2004; Afghan MP Fariba Ahmadi Kakar who was kidnapped by the Taliban in 2013; and Kenyan parliamentary candidate Flora Terah who was beaten in 2007.⁷⁹ In Peru, 41% of local counselors and female mayors have been subjected to violence.⁸⁰ A Mexican mayor, Maria Santos Gorrostieta Salazar, had been attacked several times and shared photos of her scars and colostomy bag after two attempted assassinations. Unfortunately, her attacker's third assassination attempt was successful and she was killed in 2012.⁸¹ Additionally, a Tunisian candidate was locked inside her home so her husband could keep her from actively campaigning, and a Ugandan activist was stripped naked at a party rally in 2015 by police officers.

The International Foundation for Electoral Systems (IFES) assessed online harassment of politically and civically engaged women in Bangladesh, finding “...a clear connection between online and offline abuse.”⁸² Credible evidence found that “[p]erpetrators may combine online harassment and harassment in the real world, or they may escalate from online abuse to physical and sexual violence.”⁸³ Moreover, online sexual abuse can escalate into “politically motivated rape” used to repress, humiliate, and disenfranchise women.⁸⁴ Furthermore, the “normalization of violence through TFGBV contributes to the normalization of violence against women and girls” in the real world.⁸⁵ This normalization of violence is then intensified online, as it is then seen as less harmful, serious, or dangerous to the victims.⁸⁶

In November of 2021, Arizona Representative Paul Gosar posted to both Twitter and Instagram an animation of the fake assassination of Representative Alexandria Ocasio-Cortez.⁸⁷ Such violent online posts are often done as ‘jokes’ with no thought to the real-life consequences. However, such posts can, and do, translate into real-world violence. Gosar should know this since he is from Arizona, for Arizona’s 4th congressional district Representative, Gabrielle Giffords. Giffords was shot in the head in 2011 during a public gathering. Fortunately, she survived the attack but resigned from Congress the following year due to health complications.⁸⁸ This physical, and almost deadly, attack followed significant online harassment in the weeks before the attack. Sarah Palin, a former vice-presidential candidate, posted a map of 20

congressional districts whose representatives she did not align with. The 20 districts, one of which was Giffords', were marked with a crosshair and the phrase "Don't Retreat, Instead - RELOAD."⁸⁹ Such posts can incite real violence and be a catalyst for future physical attacks.

The interlocking nature of physical violence against women and gender-based online harassment create obstacles for women's political participation due to implications for electoral integrity because "...a subset of the population is systematically excluded or blocked from participation" in the democratic process.⁹⁰ Online abuse towards women in politics can normalize and desensitize harassers to the harm done by such acts. In turn, this desensitization can be used to mobilize physical attacks. A recent survey in Malawi finds that "53.7 percent of women experienced physical abuse exacerbated by online violence and that 34.4 percent were harmed or injured as a consequence of it."⁹¹ Fear surrounding attacks against female political figures can hinder the participation of women at the public level, causing them to self-censor or remain silent altogether. Any form of targeted gender-based attack negatively impacts women's collective ability to actively and safely participate in democratic processes.

A Multinational Pandemic

The prevalence of online abuse against female political figures constitutes a truly global pandemic. From violent threats and cyberstalking to sexual harassment and the pretend auctioning of women without their consent, violence manifests itself in several forms across nations and culture. However, the objectives of perpetrators and the implications for female political figures and women's political participation find transnational common ground. This section surveys incidents involving female politicians and candidates around the world, demonstrating the universality of this issue.

In India, women are facing high levels of online abuse. As noted above, a new trend in harassment is the pretend online auction of women. Hiba Beg, a former journalist, was visiting family in New Delhi when she discovered she was "for sale" on an auctioning app for the second time in less than a year.⁹² India's auctioning apps have been targeting prominent women including politicians, activists, and journalists by uploading their images online and entering them into fake auctions.⁹³ The auctioning apps never involved any actual auctioning of people, but appears to be part of a larger conspiracy to silence the voices of Muslim women. Bulli Bai, the auctioning app hosted by Github, shared pictures of dozens of women who were vocal about

state issues without their consent.⁹⁴ The name *Bulli Bai* itself is a derogatory term that is sometimes used to describe Muslim women. These auctioning websites indicate that online abuse is not merely an individual-level phenomenon but may be organized in some cases. For women, being auctioned off and sold—even in pretense—carries the implicit threat of sexualized violence aimed at silencing outspoken women in India. Police investigations to date have inspired little confidence that authorities can effectively tackle the issue.⁹⁵ Beg mentions that due to the intensified online abuse, she began to self-censor, that is, she made sure to avoid critical posts involving the politics of Hindu nationalists.⁹⁶ Hasiba Amin, an employee of the opposition Congress party, states “What guarantees do we have from the government that tomorrow the threats and intimidation online is not going to turn into the real-time sexual violence on the streets?”⁹⁷ The online harassment experienced by women in India suggests that even self-censorship may not be enough to offer protection from harassment and even violence.

Harassment among women politicians in the United Kingdom has become increasingly common. Eighteen female members of Britain’s Parliament did not run for reelection, stating that the abuse experienced online and offline factored into their decisions.⁹⁸ Caroline Spelman, a former member of Parliament, described the online abuse experienced by female MPs as being almost always sexually charged, with constant threats of rape and references to their genitalia.⁹⁹ Another former member of Parliament, Heidi Allen, expressed her frustration with the invasion of privacy and the nastiness and intimidation she faces as an MP. She states, “Nobody in any job should have to put up with threats, aggressive emails, being shouted at in the street, sworn at on social media, nor have to install panic alarms at home.”¹⁰⁰ Additionally, in the United Kingdom, 98% of participants in an aspiring leaders program for women reported “witnessing sexist abuse of female politicians online; over 75% indicated this was a concern weighing on their decision to pursue a role in public life.”¹⁰¹ The online abuse experienced by female MPs, also, has a tendency of being very subtle in nature. An analysis of 11,543 tweets sent to UK members of Parliament, discovered digital microaggressions may be as damaging to women’s democratic representation as outright abuse.¹⁰² One tweet stated “Silly wee lassie playing at politics. You’ll have to find a job in the real world after the next election.” Another read “I can see by your face you have read my tweet. Hope you behave yourself in future.”¹⁰³ The online abuse, both overt and subtle, experienced by female U.K. MPs present real barriers to the political representation of women in the digital age, often discouraging their participation in politics.

Sweden is hailed for its high level of women's political participation, being seen as a leader in political gender equality. The Swedish Parliament has been numerically equal for nearly three decades, however, violence against female politicians is, paradoxically, increasing.¹⁰⁴ Survey data from a large number of Swedish female politicians showed that 30% of elected politicians experienced violence, harassment, or threats in 2018, up from 20% in 2012.¹⁰⁵ Survey data on local-level Swedish politicians indicates that women are particularly exposed to political violence at all levels of government (rank and file, committee chairs, and mayors).¹⁰⁶ The article finds that women politicians in Sweden are more exposed than men to offensive comments found on online forums.¹⁰⁷ Women politicians are also more exposed to comments alluding to their sexuality, focusing on their appearance and targeting them as women rather than politicians. One female MP states "Women and girls really get "online hated" in a different way that is horrible. You notice a big difference if I write a post on Facebook or Twitter compared to if exactly the same post would come from a male colleague."¹⁰⁸ Even in Sweden, a world leader in gender equality, online abuse targeting women MPs is often gendered in its content, presenting barriers to women's political participation despite the nation's leadership on this front.

The Middle East and Northern African states are known for having some of the lowest rates of women's political participation. It might not come as much of a surprise, then, that in a report by the Economist Intelligence Unit, the Middle East was found to be the region with the highest prevalence of online harassment against women at 98%.¹⁰⁹ Female politicians in Iraq, for example, have faced unprecedented smear campaigns, taking place both online as well as in person. These women are often targeted using fake sex videos that are widely circulated online; these videos show the female candidates in bed or posing in revealing outfits or underwear.¹¹⁰ Videos such as these are meant to destroy the reputation of the women and force them to withdraw from running for parliament; unfortunately, the tactic works, and some have dropped out of their races.¹¹¹ In Israel, newspapers and other media have been doctored to remove female ministers from government photographs and replaced by images of male ministers. The two women, Limor Livnat and Sofa Landver, were removed by members of the ultra-orthodox to attempt to erase them from the narrative.¹¹² The Digital Rights Foundation reports that within Pakistan, 40% of women have experienced stalking or harassment via messaging apps.¹¹³ In Egypt, 41.6% of women have experienced some form of online abuse.¹¹⁴ Egyptian women had an extremely high rate of online harassment coming from strangers: 92% of all harmful content was

sent by an unknown person.¹¹⁵ In Afghanistan, before its fall to the Taliban, almost all of the female candidates in the running for the 2010 election had been victimized by threatening phone calls.¹¹⁶ Now, of course, women in Afghanistan are not allowed to stand for election at all.

A study by Pollicy, a feminist civic tech organization in Uganda, reported on the amplified online abuse against women politicians during elections. In Uganda's 2021 general election, women in politics faced problems with the emerging spread of Covid-19 forcing Uganda's electoral commission to declare the general elections a 'scientific' one.¹¹⁷ This term meant that all campaigning was to be done digitally via radio, television, and social media. The switch to a digital election made campaigning no easier or safer for female candidates. The report discovered that online abuse in Uganda manifested in several ways, including reports of sexual harassment, offensive name-calling, and stalking as the most common.¹¹⁸ Nancy Kalembe, the only female presidential candidate, reported on an online video that surfaced referencing her "failed " marriage as a tactic to derail her campaign.¹¹⁹ In this instance, gendered disinformation was used to equate divorce for women with unsuitability for political office. Kalembe also began receiving calls from individuals claiming to be government officials urging her to drop out of the race.¹²⁰ Agness Nanduttu, State Minister of Karamoja Affairs, received comments instructing her to get married because as a single woman she is deemed incapable of leading.¹²¹ Again we see the tactic of tying suitability for political office with societal norms of "proper" behavior for women. Approximately one in three women in Uganda were victims of online abuse during the 2021 election, with 14.5% of them deactivating their social media accounts to escape the abuse.¹²² Female politicians in Uganda have resorted to using Facebook rather than Twitter to engage with voters due to lower levels of online abuse.¹²³ Female candidates reported feeling "safer" on Facebook because users were required to "friend" them or be approved into the group in order to view/comment on content.¹²⁴ However, using this tactic means women in Uganda still distanced themselves from social media allowing online harassment to affect their campaigning.

Reporting shows that in Kenya over 33% of girls have faced online harassment and 28.2% of women within these five African countries (Ethiopia, Kenya, Uganda, Senegal, and South Africa) have faced TFGBV including doxing, stalking, sexual harassment, and offensive name-calling.¹²⁵ In terms of cyberstalking specifically, 26.7% of women in Kenya, Senegal, South Africa, Uganda, and Ethiopia report experiencing this. This same group of African countries also have something in common: women from Kenya, Senegal, South Africa, Uganda,

and Ethiopia stated that a majority of their experiences with online gender-based violence occurred on Facebook.¹²⁶ A study conducted in Kenya, Colombia, and Indonesia showed that online abuse induced politically active women to pause, decrease, or completely halt their social media engagement.¹²⁷

In New Zealand, harassment against women on social media platforms has never been more evident. Currently, 60% of harassment toward female politicians comes from inappropriate social media contact.¹²⁸ Social networking sites and email are common modalities for harassing female politicians. MPs in New Zealand report death and rape threats that are made online, and online harassment has begun to infiltrate their personal, private lives.¹²⁹ These MPs have seen an uptick in harassment targeting their family members as well as themselves. Every-Palmer finds that “the use of the internet as a platform for harassment was reported more frequently than in other comparative studies and was a major concern for MPs.”¹³⁰ These findings present social media platforms as a potential safety threat for New Zealand women MPs.

In Italy, the speaker of the Chamber of Deputies, Laura Boldrini, had been harassed with various insults and violent threats, some of which call for her assault, both sexual and physical. She was sent doctored photos of her face edited onto the body of a woman being raped.¹³¹ Boldrini states “It's terrible. Sometimes they also say, 'We know where your apartment [is], we know your address'. I have a daughter. She's studying in the UK; she is 20. And when she is here I am always very anxious. Because I don't want her to have a problem because of me.”¹³²

In Bangladesh, the International Foundation for Electoral Systems (IFES) conducted an assessment of online abuse against politically and civically engaged women.¹³³ From analyzing data from public content on Facebook, Twitter, and Youtube, the report identified trends in online abuse against women in politics in five key categories: sexual violence, psychosocial violence, physical violence, homophobic violence, and religious- and ethnic-based violence and found that online abuse against women is pervasive.¹³⁴ The report identified a total of 553 posts in English and 158 posts in Bengali that contained sexual violence.¹³⁵ Threats of sexual violence were the most common forms of online abuse found against women in Bangladesh.

Canadian female politicians also face a high amount of online abuse. Christine Labrie, a member of the Quebec National Assembly, received a high volume of harassment online. The hate speech directed at her included the following phrases: “useless human being,” “prostitute,”

“get dressed or commit suicide,” and “you should disappear, you are a disgrace to Quebec people.”¹³⁶ Montreal Mayor Valerie Plante has also been harassed online for her laugh, with insults to her femininity.¹³⁷ Lenore Zann, former MP of the House of Commons of Canada, had a nude photo of herself from her days as an actress that surfaced on Twitter.¹³⁸ After a heated argument on Twitter, asking the user to delete the post, Zann began to receive hateful messages on Twitter which she describes as “the worst two weeks of my life.”¹³⁹ Rana Bokhari, former leader of the Manitoba Liberal Party, has been the victim of racist attacks, death threats, and sexual harassment.¹⁴⁰ One of Bokhari’s accounts of online harassment included a man sending a photo of his genitals.¹⁴¹ Bokhari shares that she was afraid of the backlash she would have received if she went public about these attacks, therefore, she was left to suffer in silence.

Female candidates in the U.S. experience an amplification of online harassment during political campaigns. In 2016, Erin Schrote, a congressional candidate from California, received tens of thousands of abusive messages via email, Facebook, Twitter, and Instagram, and some were sent directly to her cellphone.¹⁴² One of the messages received stated, “All would laugh with glee as they gang-raped her and then bashed her bagel-eating brains in.”¹⁴³ Another said “It’d be amusing to see her take twenty or so for 8 or 10 hours.”¹⁴⁴ Years after losing the election, Schrote continually received online harassment, showing that even removal from the political sphere is not enough and that women face harassment over a sustained period of time. Another universal theme of online harassment is that female candidates are more likely to receive online abuse than their male counterparts. An analysis of online abuse targeting Congressional candidates during the 2020 US presidential campaign showed that on Facebook female Democrats received ten times more abusive comments than their male counterparts, while Republican women received twice as many abusive comments as Republican male peers.¹⁴⁵ A report from 2016 shared similar findings when examining abusive tweets toward Hillary Clinton and Bernie Sanders. Findings showed that Hillary Clinton received abusive tweets at a rate almost twice that of Sanders.¹⁴⁶ Online abuse towards Clinton increased as her selection as the Democratic presidential candidate became more of a certainty.¹⁴⁷ With online harassment being targeted at some of the United States’ most prominent women, there is no limit to how far this abuse can go. In politics, being harassed online becomes a part of the job for some. Rebecca Thompson, a Democratic candidate in Michigan, states “I told myself I had to just suck it up — there’s no crying in baseball; there’s no crying in politics.”¹⁴⁸ What’s concerning is how

normalized online harassment against women in politics has become. Mya Whitaker, a City Council candidate in Oakland, says “It becomes so normalized, the types of things that people say. Being a black woman and existing, in some cases, is enough to piss people off.”¹⁴⁹ These forms of harassment and abuse experienced by women are often viewed as just another obstacle women have to endure if they want to try and change the system that drives it.

Additional Findings

The tale appears to be the same everywhere on the planet. In Bolivia, after reviewing ten years of case files, the Association of Locally Elected Women in Bolivia discovered that more than one-third of the complaints it received contained forced resignations, the online harassment pressured women local councilors to hand over their seats to male alternates.¹⁵⁰ This resulted in fewer women running for a second term. Moreover, they believed that holding political office was not worth the physical and psychological violence they had endured.¹⁵¹ Reporting based on data from Cote d'Ivoire, Honduras, Tanzania, and Tunisia reveals the extent to which women in politics face online harassment.¹⁵² When asked if the female politicians had experienced the following types of violence while carrying out their political party duties, 18.8% responded that they had experienced harassment online or via social media and 14.1% reported that they had experienced threats sent via social media or online.¹⁵³ The Inter-Parliamentary Union conducted a study on harassment against women in parliaments and found significant data regarding online abuse. The scope of this study involves 123 women from 45 countries in Europe, 81 of these women are MPs and 42 are on the parliamentary staff.¹⁵⁴ According to the research, “58.2 percent had been the target of online sexist attacks on social networks.”¹⁵⁵ Furthermore, electronic communication was found to be the primary means used in such threats. The messages can be extremely violent and disturbing, some include crude insults and nude images, or are targeted using pornographic videos.¹⁵⁶ Women themselves are not the only targets, “46.9 % of the respondents reported receiving messages of death threats, threats of rape and beatings, against them, their children and their families.”¹⁵⁷

Based on this survey of regions, it is evident that the problem of technology-facilitated harassment of women political figures is truly a global scourge. While the precise forms of attack may differ in some idiosyncratic ways, in most cases the modus operandi is exactly the same: sex-based threats made terrifying by doxxing, deepfakes, and online auctions. Despite these threats being online, they prove to have detrimental effects on women in politics globally. As you

can see, women are self-censoring, disengaging from politics, limiting their social media usage, and eventually removing themselves from these types of platforms.

Figure 1. A Map of Countries Examined in A Multinational Pandemic.



Effects of Gender-Based Online Harassment on Women's Political Participation

Intersectionality Matters

Researchers find that gender-based online harassment does not affect all women equally: intersectional identities, such as race, ethnicity, sexual orientation, religion, gender identity, and political affiliation, are significant exacerbating factors. This is troubling because the hallmark of democracy is its inclusion of all citizens, regardless of identity, into political life. Diversity, equity, and inclusion are important priorities in democratic governance. Democracy is jeopardized when such principles of equality and equity are undermined by incidents of targeted online harassment. Coupling the targeting of minorities with the targeting of women on an intersectional basis is doubly corrosive to democracy, then. Harmer and Southern analyzed tweets sent to British female MPs in their article on online microaggressions, finding that Black women face the highest levels of abuse compared to their colleagues.¹⁵⁸ A report by Amnesty International tracked Twitter abuse against female members of Parliament during the 2017 UK

general election. Diane Abbott, the first Black woman elected to Parliament, received nearly half of all the abusive tweets examined overall by Amnesty International.¹⁵⁹

Indeed, numerous studies demonstrate that women of color in parliaments appear to be subjected to even higher levels of online abuse during the time of elections. In a sample of 778 women, Amnesty International's data revealed that "black women journalists and politicians within the US and UK were 84% more likely to be the target of hate speech online compared to their white counterparts."¹⁶⁰ Researchers Francisco and Felmlee find that Twitter messages sent to women of color were the most harmful and aggressive as compared to white women.¹⁶¹ Messages to Black women focused on themes of promiscuity, and Hispanic/Latine women were sent xenophobic messages, commonly referring to menial labor or relating to building 'the wall.'¹⁶² Human Rights and security expert, Marie Lamensch highlights that women of color are 34% more likely to experience online harassment compared to their white female counterparts in politics and positions of leadership. Not surprisingly, women who are in an ethnic minority are much more likely to be attacked using racialized and discriminatory language.¹⁶³ In India, one in every seven tweets was "problematic or abusive" and female politicians who were Muslim or belonged to marginalized castes "...received substantially more abuse..."¹⁶⁴ Harassment and violence are heightened for women if they "...have a disability, are racialized, LGBTQIA+, socioeconomically disadvantaged..." and harassment is worsened if they are more politically outspoken.¹⁶⁵ Gender-based online harassment exploits social inequalities as women from non-dominant ethnic, racial, sexual, or religious minority groups will be targeted differently.

Gendered disinformation campaigns further exploit these differences in identity. As stated above, gendered disinformation is "a subset of online gendered abuse that uses false or misleading gender and sex-based narratives against women, often with some degree of coordination, aimed at deterring women from participating in the public sphere."¹⁶⁶ A recent example of these stigmatizing narratives can be seen in the analysis of claims made about Vice President Kamala Harris; following her nomination as VP, false claims were being shared about her on Twitter approximately 3,000 times per hour.¹⁶⁷ Some of the false narratives shared included questioning her eligibility to be vice president due to her immigrant parents, doubting her Blackness, or questioning if she had slept her way into the position.¹⁶⁸ These narratives target her sexuality and her race. Such claims and rumors draw on misogyny and act to delegitimize not

only her but other women who are in politics and the public sphere, fundamentally exemplifying a gendered disinformation campaign.

Intersectionality also affects women's online harassment via algorithm biases. Algorithms and machine learning take on the implicit biases of the software developers. As such, the "systems can be biased based on who builds them, how they're developed, and how they're ultimately used."¹⁶⁹ If the data these systems and algorithms are trained on are not complete, balanced, accurate, and fair, this will lead to negative bias in the algorithm. These systems thereby learn how to be racist and sexist. One study found that as a computer system learns English, it will become biased against women and Black Americans.¹⁷⁰ Tangible effects of this can lead to algorithms suppressing female candidates from searches by preferencing white males in search results.

Women of color, women in minority religious groups, women in the LGBTQ+ community, and other groups who are involved in the political arena will be targeted more severely than their counterparts. Higher rates of online harassment can yield higher rates of fear or discouragement. Women from already marginalized groups will experience inordinate impacts creating greater hindrances to said women's political participation. Self-censorship and even self-removal of women as a result of these attacks undermine the potential contributions women who are members of marginalized groups can and do make to public discourse.¹⁷¹ Looking into the intersectionality of online harassment is important to fully understand the scope of the issue. Minority groups are disproportionately impacted and the harassment is cross-cultural; different countries will have different minority groups that are the primary targets. Hate and harassment are not equally distributed.

Levying Heavy Costs on Political Engagement

While research on how female political figures respond to online harassment is still in its infancy, a few generalizations can be gleaned from the literature. The political advisory firm Atalanta finds that female politicians are often distracted from their work as a result of the harassment.¹⁷² They may have to spend as much or more time on threat mitigation as on campaign strategizing. This **time-and-energy cost**, though invisible, can have debilitating effects on the success of a politician. In addition, the harassment may cause them to fear for their safety as well as that of their families, especially as the online attacks can be extremely graphic and

life-threatening. There is thus an **emotional cost** to being a woman in politics, where stress due to fear may be significantly heightened. Encouraging and supporting women to pursue a career in politics means nothing if they cannot conduct their campaign and duties without fear of online abuse. While there is a space for women in politics, it is not a safe one.

Such justifiable fears may lead to the need to acquire and pay for a dedicated security team. CTV News, a top Canadian news channel, reported that Canadian Environment Minister, Catherine McKenna, was pushed to increase her security detail due to an influx of online threats and verbal harassment in public.¹⁷³ Such security often comes with a hefty price tag. There is thus a **financial cost** involved in mitigating the insecurity felt by female political figures. The power of online harassment has led female politicians to drop out of their races altogether. In a sense, this is a steep **political cost** of harassment. Kim Weaver, an Iowa Democrat, pulled out of the race against Representative Steve King after the far-right media released an article titled “Meet the Whore Who’s Running Against Steve King” and others showed up at her home and placed “for sale” signs in the front yard.¹⁷⁴ In Malawi, 225 out of 425 women running for office in 2009 quit before the end of the election due to intimidation and online harassment.¹⁷⁵ In more extreme cases where online harassment leads or threatens to lead to physical violence, female political figures have had to move houses, adopt security measures, or leave politics altogether.

Online public engagement for female politicians may become limited and ineffective due to online harassment, representing a **communication cost**. As a result of constant online harassment, female political figures have been forced to adapt their communication strategies. Some female political figures simply post their messages and do not respond to any communication from citizens.¹⁷⁶ As mentioned in the section on Ugandan politics, female political candidates were limited to using only Facebook because it allowed them to choose the people who could engage with their messages.¹⁷⁷ Choosing a specific platform, like Facebook, to engage with voters provides a barrier of protection from strangers who could send abusive messages. To avoid online harassment, some other female political figures choose to not discuss certain topics that might cause an unwanted response.¹⁷⁸ Women have to self-censor online and often adapt their campaign and political strategies to mitigate the harm of online harassment.

However, in surveying these costs, it must be noted that often women are willing to pay them to have a political voice. In a study of female Canadian politicians, Wagner finds that women’s political ambitions generally did not waver in response to online harassment.¹⁷⁹ The

politicians in this study indicated they have acknowledged such harassment as an inevitable part of the political environment. One female politician stated that online harassment would not deter her from running for election but is something for which she would “have to prepare.”¹⁸⁰ As we have seen amongst responses to the heavy costs of online harassment, this may involve mental, emotional and financial preparation. The effect is not specific to Canada. In our interview with Josefina Erikson and Cecilia Joseffson, experts in the fields of gender and politics, they asserted that Swedish female members of parliament also interpret the rampant online abuse as a part of their job, and therefore it does not significantly change their behavior. Online harassment is equated to an everyday occurrence that no longer surprises women.

The More Women, the Greater the Outrage

One could assume that having more women in political positions might increase societal levels of gender equality, thus reducing levels of harassment over time. While there are no long-term studies, short-term studies suggest this is not the case; in fact, the reverse might be true. Matfess et al. highlight that the rise in political violence amongst citizens in Kenya was attributed to the increase in the representation of women in the country’s legislative government.¹⁸¹ Originally thought to be a move that would ameliorate conditions for women in the country, having more women in political positions increased outrage as many people would not accept such change that went against social norms for women. The unwelcoming environment inhibits the positive change that could arise from a government with an equal distribution of men and women. Political persuasiveness is stifled because female political figures do not engage in discussions with people who may have further questions.

Effects on Democracy

A decline in the political ambitions of women may represent a sign of democratic backsliding. Rather than a democracy becoming more representative of its citizens as all are welcomed into the political process, democratic backsliding suggests that over time democracy is becoming *less* representative as segments of the population are pushed out of the political arena. While women are not the only segment of society this has affected, they are the most openly and brazenly attacked and thus serve as a bellwether for the state of mutual toleration in a democracy. Marie Lamensh, the Project Coordinator for the Montreal Institute for Genocide and Human

Rights Studies, has interviewed female political figures who have stated they would have not entered the public eye if they had had prior knowledge of the level of online harassment they would experience.¹⁸² Lamensh highlights the experiences of Tamara Taggart, a former political candidate who was quoted as saying, “I would never, ever, ever subject myself to that again” about her experiences with online harassment during her federal election campaign.”¹⁸³ As we have seen, such experiences are not singular to one election or even to one country. Amnesty International reports in their 2020 “Troll Patrol Project” that female political actors in Britain and the United States receive an abusive message on Twitter every 30 seconds.¹⁸⁴ In a similar study by the National Democratic Institute, female political actors in Kenya, Colombia, and Indonesia were recorded interacting less frequently and even terminating their Twitter accounts as a result of the online abuse.¹⁸⁵ Social media is a vital platform for political actors to engage with their supporters and potential voters. Female political actors are being pushed away from online public engagement due to rampant online harassment which stifles their campaign and may damage the relationships they have built. The silencing of women in online forums does not suggest equal opportunity in a democratic society.

Indeed, engagement in political discussions—or a lack of such engagement--can also be a useful measure of the extent to which online harassment affects an individual. Lilleker et al.'s study on France, the United States, and the United Kingdom suggests gender is a key determining factor in the level of engagement with political content.¹⁸⁶ Women will engage less with political content because online harassment¹⁸⁷ has trained them to not respond until they have become competent on the topic.¹⁸⁸ Engagement such as commenting on, or even sharing, political content occurs at a lower frequency for women compared to men. This cautious behavior by women has been found to extend to women who do not have personal experiences of online harassment. That is, the looming threat of online harassment preemptively steers them away from greater political engagement due to fear.¹⁸⁹ Barker notes a paradox of online harassment against women: while the harassment against women in politics is highly visible, the voices of the victims become increasingly invisible.¹⁹⁰ The high visibility of the abuse legitimizes society's acceptance of online abuse against women while silencing the victims at the same time. This phenomenon could be equated to authoritarian tendencies, for the subjugation of women through violence, both physical and online, has become normalized in some settings. The increase in online harassment of women in politics makes the internet a hostile space for all

women, not just those in politics. If the public square is increasingly an online square, then women's hesitancy to express opinions online matters for those who seek to promote democracy.

Furthermore, while we have concentrated on female politicians in this literature review, some important female political actors are not politicians, but also suffer the same harassment. *Malign Creativity* determines online harassment is a major issue for all female political actors, including journalists, civil rights activists, and politicians.¹⁹¹ In the last ten years, female journalists have reported an uptick in online harassment attributed to the popularity of social media.¹⁹² Female journalists are under threat for simply doing their job. Online harassment interfering with their work brings into question whether freedom of speech and freedom of the press is being upheld. Similar to journalists, civil rights activists are political actors that rely on social media for their type of work. Civil rights activists document injustices occurring throughout society and within the government. By silencing female journalists and civil society actors, online harassment erects barriers to citizens becoming aware of abuses of their rights. This undercuts the democratic purpose in having a free press. A strong democratic society would ensure female political actors in all their various vocations can conduct their work without fear of harassment, or at the very least make efforts to get to that point.

Existing Policies and Programs

Governments and regulatory entities have made commitments to prevent and punish the online harassment of women, but only to a certain extent and with only limited enforcement. Because this issue is relatively new, and just now being acknowledged by governments, most governmental action currently consists of making verbal or written commitments to improve the situation for women. Furthermore, the extent of governmental acknowledgment of the problem differs by region. Regions like the Middle East and Africa are largely missing any legislation or verbal/written acknowledgment of the issue, outside of nongovernmental organizations (NGOs). There is limited governmental recognition of women's physical security in these regions, even without technology being involved, so we would expect a similar low level of acknowledgement for online harassment.

However, the beginnings of an action agenda are becoming visible in countries across the globe. The general actions and commitments made by countries that recognize the issue will be

described below, alongside NGO contributions. Subsequently, the recommendations of scholars surveyed in this literature review will also be examined. This overview should shed light on the possibility of multilateral and coordinated action that might potentially emerge from current initiatives.

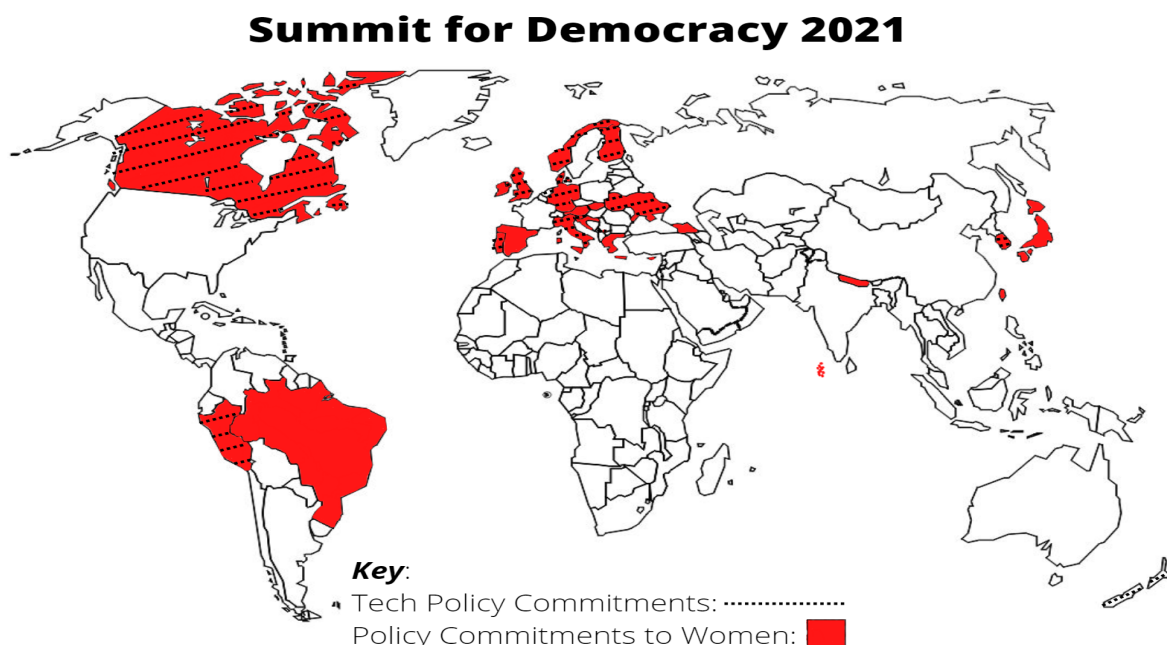
Major Trends in Regional and Country Responses to Online Harassment

Major trends in regional and country action in response to this phenomenon include:

1. Greater recognition that the exclusion of women from the political sphere due to online harassment undermines democratic governance.
 - This recognition can be seen, for example, in the promulgation of initiatives focused on democracy enhancement in the U.S. and its Summit for Democracy partner countries
2. Enhancing legislation on gender discrimination to include online harassment in Latin America, and
3. Data protection and online safety initiatives in Europe

We will discuss each trend in turn.

Figure 2. Map of Summit for Democracy Countries that made policy commitments involving technology and/or women's rights.



Greater recognition in democracies

Concerning the first major trend, the U.S. is planning to host its second Summit for Democracy at the end of 2022 where countries will likely continue to make commitments that address the online harassment of women and women's political empowerment. Note that the Summit for Democracy is by invitation only, and if the U.S. wants to push these initiatives with countries that struggle the most with women's online harassment, additional work will have to be done outside of a democracy-focused conference. The U.S. government is beginning to acknowledge how detrimental the online harassment of women, particularly women in politics, is to the preservation of democracy. In last year's Summit for Democracy Proceedings, for example, Ambassador Katherine Tai, the US Trade Representative, "...announced several new U.S. programs focused on gender equality and democracy, including the \$33.5 million Advancing Women's and Girls' Civic and Political Leadership Initiative (pending availability of appropriations) and the Global Partnership for Action on Gender-Based Online Harassment and Abuse, which will be launched in partnership with the Government of Denmark."¹⁹³ These two initiatives are at the forefront of United States and multilateral efforts and democratic country action.

The Advancing Women's and Girls' Civic and Political Leadership Initiative seeks "to strengthen women-led civil society organizations, tackle entrenched barriers to women's political and economic participation, and foster a more inclusive environment for women in politics."¹⁹⁴ As previously stated, without data collection on women's online harassment and its concomitant impacts on female political figures, effective policymaking will be almost impossible. The Advancing Women's and Girls' Civic and Political Leadership Initiative will be led by USAID and the Department of State. Specific lines of effort for this initiative include:

- "S/GWI's Supporting Her Empowerment: Women's Inclusion for New Security (SHE WINS) initiative plans to provide local, women-led civil society organizations with grants and technical assistance in Africa, the Middle East, and North Africa, and South and Central Asia.
- ...The Bureau of Democracy, Human Rights and Labor (DRL), in collaboration with S/GWI, is planning to launch SHE PERSISTS, or Supporting Her Empowerment: Political Engagement, Rights, Safety, and Inclusion Strategies to Succeed. SHE PERSISTS is intended to work with public and private sector partners to provide funding for technical assistance on advancing women's safety, political participation and empowerment, and initiatives for inclusive democracy. Including the

development of National Action Plans to End Gender-Based Violence (GBV) and small grants to local organizations working to address barriers to women's political and economic participation, including violence against women in politics, online harassment and abuse; countering disinformation and democratic backsliding, economic harm and isolation, encourage women in all their diversity to participate fully in democratic processes; and support young and emerging women leaders to seek political office or other public leadership roles.

- The U.S. Agency for International Development is planning to initiate the Women's and Girls' Civic and Political Leadership program. In partnership with like-minded governments, the private sector, civil society organizations, and multilateral institutions, the project is expected to take an ecosystem approach, empowering women and girls interested in politics while creating a more inclusive environment for their representation in up to 10 focus countries. Through this activity, USAID and implementing partners are planning to offer skill-building for women and girls, encourage legal reform for women's participation, work alongside male allies to support women's political leadership, and combat violence against women in politics and public life.”¹⁹⁵

These initiatives appear to be a great starting point for reinforcing these values in developing countries, especially through aid programs geared towards women. Since there is also little data on Africa and the Middle East on women's online harassment, S/GWI has an opportunity to collect this data through the initiative. The technical assistance portion of the initiative is crucial, as elections and democracy become more affected by online content. Helping women become as literate as possible when it comes to online content can also help protect them from online harm. This technical assistance can likely include helping the women make their online campaigns in a way where they can vet those who view the content. These are all initiatives that S/GWI should be looking at when considering how to teach women to be defensive against online harassment, as well.

President Biden committed to bolster the Advancing Women's and Girls' Civic and Political Leadership Initiative, including convening a national task force on online harassment and abuse that will combine

“...federal agencies, state leaders, advocates, law enforcement, and technology experts to study rampant online sexual harassment, stalking, and threats, including revenge porn, deep fakes, and the connection between this harassment, mass shootings, extremism and violence against women. The Task Force will be

charged with developing cutting-edge strategies and recommendations for how federal and state governments, social media companies, schools, and other public and private entities can tackle this unique challenge. The Task Force will consider platform accountability, transparent reporting requirements for incidents of harassment and response, and best practices.”¹⁹⁶

Though no information can currently be found on this national task force, or whether it has even been established, there is information on the Biden Administration’s establishment of the White House Gender Policy Council, which seems to, broadly speaking, be addressing the issues listed. The White House Gender Policy Council was and is facilitating the aid and planning going into the Global Partnership for Action on Gender-Based Online Harassment and Abuse along with the Advancing Women’s and Girls’ Civic and Political Leadership Initiative.¹⁹⁷ However, those are the only two programs we have identified that have claimed to be working on technology-facilitated gender based violence.

Two years later, it appears that little has been done to create these “cutting-edge strategies.” Much of these initiatives appear to be a combination of rhetoric plus some funding to support entities already working in this space. However, we cannot find information on whether any of the funding pledges have been fulfilled, or funding allocated. Biden’s campaign promises also included further funding to bolster law enforcement agencies from the local to federal level in order to give them more bandwidth to pursue investigations into “...online sexual harassment, stalking, and threats while also supporting victims.”¹⁹⁸ Since coming into office, the promise of increased funding seems to have been kept, as spikes in funding for police forces have been seen all across America with Biden’s support.¹⁹⁹ However, there is no available information at all as to whether or not this increase in funding correlated to a more active law enforcement when it comes to online harassment or abuse against women, or female politicians, specifically. A system to establish accountability or even benchmarks for these goals is completely missing.

The Global Partnership for Action on Gender-Based Online Harassment and Abuse, led by the U.S., as part of a coalition with Denmark, Australia, Sweden, the Republic of Korea and the United Kingdom, specifically targets technology-facilitated

gender-based violence, and has, so far, created a brief roadmap to get countries to the right policies and practices to address the issue. The roadmap lays out three primary objectives:²⁰⁰

1. Develop and advance shared principles,
2. Increase targeted programming and resources, and
3. Expand reliable, comparable data and access to it

This partnership is new, started in 2021, and we hope some of the policy and action recommendations brought to light in this paper can provide more specific action to meet these objectives. The objectives of the Global Partnership were just recently published, on March 16th of this year, and so details of specific programming are currently lacking. These initiatives seem to be in their early stages and lack any outline of what direct action might meet these objectives, at least based on a search of the open source literature. These action programs—assuming they come into existence--will be important to track, for they will become the starting point for developed, democratic countries to address these issues for themselves. However, it will be crucial to collect systematized, standardized data on the current baseline of what is happening *prior* to these actions being taken, so that proper evaluation of the difference these programs make can be assessed. In addition, as noted previously, the U.S. should consider how it can start this same dialogue with countries that are non-democratic or are developing democracies to address this issue

Australia has a comprehensive eSafety Commissioner Program, and they are also part of the Global Partnership. Their participation can be leveraged to show other countries how the Australian program works, and facilitate similar programs in other Partnership countries. The eSafety program in Australia is the first “government regulatory agency committed to keeping its citizens safer online”.²⁰¹ It is headed by a Commissioner who executes action that this government entity can take under the Online Safety Act 2021. The Online Safety Act allows this branch to do the following:

“The Act enhances our ability to act quickly to protect victims of online abuse across our reporting schemes. It gives us the authority to compel online service providers to remove seriously harmful content within 24 hours of receiving a formal notice – halving the time previously allowed (though eSafety may extend this period in certain circumstances). The Act stipulates what the Australian Government now expects of technology companies that operate online services.

The Act also requires the industry to develop new codes to regulate illegal and restricted content. This refers to the most seriously harmful material, such as videos showing sexual abuse of children or acts of terrorism, to content that is inappropriate for children, such as pornography”.²⁰²

The eSafety program also includes:

“A world-first Adult Cyber Abuse Scheme for Australians 18 years and older, across a wide range of online services and platforms. A broader Cyberbullying Scheme for children to capture harms that occur on online services and platforms other than social media. An updated Image-Based Abuse Scheme to address the sharing and threatened sharing of intimate images without the consent of the person shown. Targeted powers to require internet service providers to block access to material showing abhorrent violent conduct. Stronger information-gathering powers. A modernized Online Content Scheme to regulate illegal and restricted content no matter where it’s hosted, bringing in app distribution services and search engines”.²⁰³

These initiatives can also be bolstered by targeting gender-specific online harassment, especially instances involving women in politics. Since the eSafety Program also includes multilateral action with tech companies, this approach can be a good template for other countries to initiate a similar dialogue with these companies, especially social media entities. So far, this initiative has been excellent at pointing out flaws in the effectiveness of enforcing Australia’s eSafety laws, and the current Commissioner has reported about the reality of social media’s sites inability to adhere to government regulations.²⁰⁴ An examination of what the eSafety Commissioner has not been able to do would be an important topic of discussion for the Global Partnership as it seeks solutions. Furthermore, the eSafety program is the perfect entity to initiate government data collection on the effectiveness of regulation and the realities of social media company adherence. One of the most prominent policy recommendations to be addressed is the issue of data collection. This eSafety Commissioner framework creates a formal line of effort to start this data collection: the Australian commissioner is responsible for this data collection, as discussed above, but the program is so new that no public reports have been published yet.

Denmark’s Technology for Democracy Initiative is also worth watching. It is centered around global information sharing on the issues pertaining to technology and

democracy. Last year, the Initiative's conference hosted talks and forums that opened up the floor for discovery of new initiatives and ways to pursue policy to advance online literacy and protect democracy and human rights as these concepts pertain to the internet and rapid technological development.²⁰⁵ The Tech for Democracy website notes that "In June 2022, a high-level physical conference in Copenhagen takes stock of the progress made and provides a platform for raising commitments to strengthen digital democracy as a stepping-stone to the US Summit for Democracy."²⁰⁶ This second conference will be the first step to keeping tabs on the countries that made commitments to address these issues previously in the 2021 Summit for Democracy. The Tech for Democracy Initiative centers around a pledge to make a difference on this issue, which is why Denmark has committed to bolstering the U.S.-led Global Partnership for Action on Gender-Based Online Harassment and Abuse. The Tech for Democracy Initiative aims to facilitate these conversations and give countries a forum to share what they are doing to address these issues. But as the reader can imagine, it's a long way from high-level conferences to effective action, regulation, and accountability.

Enhancing Legislation on Gender Discrimination in Latin America

The second major trend we identified in this space concerns improving laws against gender discrimination to cover online space. In Latin America, efforts are being made to redefine technology-facilitated gender-based violence and online harassment against women as a form of criminal violence punishable by law. Bolivia currently leads in such legislation: Law 243, passed in 2012, specifically condemns harassment and political violence against women.²⁰⁷ In a report on gender and political violence in Latin America, more details on the law are given: "Penalties include two to five years of prison for political harassment, three to eight years for physical or psychological violence, and the prevailing sanction for sexual assault according to the criminal code. Aggravating factors that may increase these penalties include:

1. acts committed against a pregnant woman, someone older than 60, with limited education, or with a disability
2. acts committed by a person in a leadership position in a political party, a citizen movement, or the public service, or if the person has recommitted acts of political harassment or violence against women; and
3. acts committed by two or more people.

State parties responsible for implementing this law comprise the ministry of justice, the electoral authorities, and leaders at different levels of government.”²⁰⁸ Though the law mentions the terms political harassment and physical or psychological violence, these terms are not defined in the law, nor is there a list of what crimes fit into these categories. Carley Clontz, a student researcher at the University of Pittsburgh, notes that Bolivia struggles with enforcing these laws, and many cases go unrecognized as falling under Law 243 even 10 years after its passage. Unsurprisingly, there is a disconnect between the law and its implementation, as is so often the case concerning women’s issues. In Bolivia’s case, cultural norms against women led to the police force not enforcing these laws, which makes the legislation of very little real value to women.

During the expert interviews we conducted with Caroline Hubbard, Senior Gender Advisor at USAID, and Julie Denham, Senior Advisor, Elections and Political Transitions at USAID, they pointed out that Mexico has undertaken major legal reform along these lines as well, and has criminalized violence against women through physical and online threats, even going as far as disqualifying perpetrators from being able to run for office. This has been put in place to have an impact on male politicians attacking female politicians or having others do so for them, occurring in Bolivia as well, but nothing noticeable has come of these laws. Unfortunately, similar to Bolivia’s inability to enforce its law, Mexico deals with the same issues. Male-led police units did little when “a female candidate for municipal president, Guadalupe Ávila Salinas, was shot in broad daylight in 2004 by the sitting municipal president while she was holding a meeting with women from the community.”²⁰⁹ We have little reason to believe that online harassment or technology-facilitated gender-based violence as it pertains to female politicians will be given the attention it deserves or the enforcement required under the new laws like Law 243 in Bolivia.

These new laws have led to no discernible improvement because corrupt governments/police forces and cultural norms that perpetuate the dehumanization and violence against women in Latin America stifle enforcement. Legislation is the first step, but it is not effective without enforcement. Turning around non-enforcement is a long-term issue that involves complex guiding tactics and likely will need active, “boots on the ground” NGOs to do some of the heavy lifting. Since making law enforcement effective involves changing the cultural perception of women, grassroots efforts must be part of the effort as well. There is an underlying

dehumanization of women that triggers impunity for violence against women, and legislation is important because it needs to be in place first before perpetrators can be appropriately dealt with.

Data Protection and Online Safety Initiatives in Europe

The third major trend, that of approaching the problem through data privacy and online safety legislation, is important but also fraught. It is important to note that the central issue governments face when passing protective legislation to combat online harassment is the potential for these same tools to be used for online censorship. The internet provides individuals with a medium to exercise their right to free speech, but when protective legislation becomes too restrictive it prompts public outcry, such as in the case of the UK's Online Safety Bill, which is discussed below.

In addition to the United States and Latin America, European policy is making efforts to prioritize data protection in its technology-based policies. This trend of enhanced data protection in European policy can be seen in the passage of the European Union's General Data Protection Regulation, the German Network Enforcement Act of 2017, and the newest and most controversial UK Safety Bill. We will discuss each in turn.

The EU's General Data Protection Regulation (GDPR) was put into effect in May 2018 and became one of the most protective pieces of cyber legislation in the world and currently acts as the pinnacle of extant data privacy initiatives.²¹⁰ This new data protection initiative for the European Union classifies "the protection of natural persons in relation to the processing of personal data as a fundamental right."²¹¹ The GDPR sets guidelines and standards for the collection and utilization of personal data for the EU. Ultimately, this legislation prohibits marketing companies from buying and selling private end-user data collected by third parties, such as social media apps like Facebook, and Twitter. The GDPR acts as a framework in which governmental actors can govern cyberspace to provide better protection for their citizens' overall privacy. In the first year after the GDPR went into effect, the European Data Protection Board reported that there were "205,000 cases reported to EU supervisory authorities and other data protection watchdogs."²¹² Many of the companies being challenged to meet GDPR regulations are US companies such as Google, Facebook, Apple, Netflix, Spotify, and more. Many of the companies have implemented compliance programs in order to adhere to GDPR guidelines in order to avoid serious penalties. We argue that the GDPR approach--enhancing data protection

and enforcing compliance through monetary penalties--can set a precedent for creating a system of legal penalties in response to instances of online harassment targeted at women

Furthermore, this legislation is unique in that it transcends national boundaries and applies beyond just the European Union, providing protection for EU citizens from international companies outside of the EU. We interviewed Min Kyriannis, cybersecurity professional and tech-startup CEO, who strongly recommends that the United States utilize the GDPR as a framework for U.S. policy to combat gender-based online harassment, particularly its enforcement capabilities. She urged that the lack of action to combat online harassment is due to the inability to enforce cyber legislation, and cited the GDPR and its strict penalties of fines up to up to 20 million euros or 44% of the firm's global annual revenue, whichever amount is higher, as a possible solution for U.S. policymakers (GDPR 2016).

In addition to the EU's GDPR, there is also action at the nation-state level. Nations are learning from each other in this sense. For example, the German Enforcement Act of 2017 lays the foundations for the more recent UK Online Safety Bill. Similar to the GDPR, the German Network Enforcement Act was one of the first protective pieces of state-level legislation to combat online hate speech but has also been dubbed the "German model for online censorship."²¹³ This legislation was created to protect citizens from online harassment, but has set a precedent that authoritarian regimes might exploit to censor free speech.

This law was originally catalyzed by a wave of hate speech targeted at immigrants during the 2015 surge of immigration into Germany. Heiko Maas, the German president at the time, demanded stricter policing by Facebook of content that violated German hate speech law, resulting in content deemed illegal in Germany being removed from the site. The demand for such action later became official policy under the German Network Enforcement, which pushed liability onto Facebook to remove content deemed illegal in under 24 hours or face penalties of up to \$55 million.²¹⁴ Since this policy has been enacted, Venezuela, Vietnam, Russia, Belarus, Honduras, Kenya, India, Singapore, Malaysia, the Philippines, France, the United Kingdom, and Australia have introduced similar policies of pushing liability onto tech companies. It is important to realize that five of these nations are deemed as 'not free' according to Freedom House.²¹⁵ That latter figure is what worries critics. What was initially instated as protective legislation to curb hate speech provides the ability for autocratic governments to repress political dissonance.

Both the GDPR and German Network Enforcement act have provided a springboard for the newest and most protective legislation: the UK Online Safety Bill, currently being debated in Parliament. Prior to the UK Online Safety Bill, a Digital Services Act for the EU had been proposed in 2020 and recently passed in 2022: it “explicitly recognizes the systemic harms that digital platforms may cause and places greater obligations on large online platforms, to regularly assess and respond to risks that stem from the use of their services.”²¹⁶ In addition to taking a similar stance, the UK Online Safety Bill further requires platforms such as Facebook, YouTube, Twitter, and Instagram to remove content that is not illegal but is deemed harmful. Just what that might mean is up for debate. The extensive ambiguity surrounding this legislation creates possible consequences such as delegating the task of determining what qualifies as safe and harmful for all end-users to the internet Silicon Valley tech giants, which delegation in turn threatens free speech.²¹⁷ Currently, the Online Safety Bill is still being debated in parliament, specifically what constitutes ‘legal but harmful’ content. This legislation does have the potential to crack down on instances of online harassment of female political figures, such as when MP Maria Piller was cyber flashed, receiving unsolicited pictures of male genitalia, while on a train to London. If the new bill were passed, it would allow for cyber harassment to be viewed with the same scrutiny as in-person harassment. Equalizing these crimes, whether perpetrated via the internet or in person, allows for accountability and law enforcement. With MP Piller’s current political status she has received an increase of “regular bombardment of online verbal abuse, death threats, and even rape.”²¹⁸ The Bill also demands tech companies provide remedy procedures, with financial penalties for inaction or delayed action to remove harassing material.

Europe’s various initiatives to increase protections for all end users of the internet have shown that there are existing frameworks that can be utilized to help protect women from online harassment. Currently, however, these are not written in a way that specifically targets gender-based online harassment. They should. We recommend the various task forces associated with these laws and initiatives begin to concretely address this issue.

Non-State Actors and NGOs Respond to Online Harassment

In addition to governments, non-state actors have also taken the initiative to combat this growing scourge. Social media companies such as Facebook, Twitter, and Google have pledged

to tackle online abuse and increase women's safety on their platforms through enhanced safety mechanisms. Not surprisingly, however, they neglect to provide actual details on these safety mechanisms. For example, Nora Lindström, the Global Lead for Digital Development at Plan International, points out that Facebook does not differentiate between gender-based online abuse and non-gender-based online abuse, which is surprising given the issue cannot be fully addressed without making this distinction.²¹⁹ Not recognizing the nuances around sex relations and how women are consistently dehumanized and experience violent treatment due to this, will not allow for effective policy to be created. The abuse specifically targeting women then goes unidentified, and unrecognized, leaving a massive data gap and a massive information gap.²²⁰ Moreover, there is overwhelming evidence that social media like Twitter treats sex-based harassment as being less inflammatory than harassment of minority groups. You can get away with rape threats on Twitter, while you can be permanently banned for misgendering an individual, for example.²²¹ If sex-based harassment is viewed as trivial, how can anything actually be done to address it?

Part of the problem may stem from technology's masculinist origins, which perpetuate a lack of concern from tech creators. After all, all large social media companies were founded by men. If these companies refuse to acknowledge how sexed this issue is, it may be almost impossible to make enforcement a reality. In addition, Nina Jankowicz, Senior Advisor at the Centre for Information Resilience, notes another problem of leaving the action to tech corporations: it is very difficult to hold these entities accountable—even for implementing their own policies. For example, Germany and Australia both have implemented programs that will fine private companies if the illegal content is not removed within 24 hours.²²² In her recent review of the effectiveness of Australian tech laws, the Australian eSafety Commissioner has found that this legislation is nearly impossible to enforce, however.²²³ We cannot find any evidence that these governments are tracking complaints and ensuring the information is removed at all.

As a result of this less-than-optimal situation, enterprising private entities have begun to supplement the efforts of governments and other companies. One example is ParityBot, made in Canada.²²⁴ Areto Labs, the company that created the AI ParityBot, describes its actions thusly: “companies can choose which accounts and hashtags to monitor, log in to their real-time data and analytics dashboard, see which reps and employees are being attacked or lauded online, and make informed mental health and digital wellness decisions based on the numbers. Areto Ally,

another bot, automatically responds to hate speech directed at your chosen social media accounts with supportive or educational messages in your brand voice. This allows you to protect your team's mental health and security and show that your brand is a true ally".²²⁵ Because this software allows companies to identify and monitor online harassment data, companies can begin making the right decisions when it comes to getting their team members the mental and physical help they need after online attacks. The creation of these types of bots were a focused, actionable step to approach the issues women in politics face online every day. Why are these private solutions getting so little attention? Alberta Tech, a platform that discusses technology in Canada, discusses the issue here:

“Areto Labs co-founder and COO Kasey Machin didn't start out in the technology field. Her start-up journey began years ago from her observations of how online toxicity was dissuading women from running for public office, adding to the existing gender gap at all levels of government. This issue was the catalyst for the creation of ParityBOT, a Twitter bot built to send positive tweets in response to negative and abusive messages sent to women running for public office. Rather than attempting to go after the senders of negative tweets, ParityBOT counters online noxiousness with a positive retort of inspirational quotes and messages of affirmation.”²²⁶

Businesses can purchase these bots to protect their workers, which raises the question of why the algorithms of larger companies such as Facebook and Twitter are not yet capable of swiftly and correctly identifying online harassment against women. There are obvious data gaps and tracking these incidents of harassment seem to be difficult for big tech companies, but much smaller private companies have made a business out of doing this exact thing. That seems to indicate that it is not as hard as the big tech companies are making it out to be. Moonshot, another private company that does online monitoring of harassment for government and private clients, tracks incidents in over 30 languages, maps them out, and provides actionable steps for companies to pursue in order to counter these threats.²²⁷ However, the actions and countermeasures are only available to paying clients. There is something to be said, though, about leveraging these technologies in order to formulate policies and lines of effort by governments that could protect citizens as part of the government's due diligence.

For-profit companies aside, NGOs have also played an important role, and sometimes the only role, when it comes to addressing technology-facilitated gender-based violence in MENA and Africa as a whole. While there is little to no evidence of governmental action in the Middle

East and Africa, NGOs in that region are working to actively fight this phenomenon. For example, Mobilizing for Rights Associates (MRA) Women, based in Morocco, has created community-based educational programs and workshops to help counter technology-facilitated gender-based violence, and they also survey the experiences of the women who experience technology-facilitated gender-based violence to get a greater understanding of how to address the issue.²²⁸ MRA Women understands the goal is long-term cultural change, but in the meantime they were able to push for legislation adopted by the Moroccan government in 2018 that criminalized certain types of technology-facilitated gender-based violence. In a news report from Al Jazeera in 2018, it was clarified that “...the legislation also declares the definition of sexual harassment, including unsolicited acts, statements or signals of a sexual nature, delivered in person, online or via telephone... Those found guilty of violating the law face prison terms ranging from one month to five years and fines from \$200 to \$1,000.”²²⁹ Though this legislation is great news and represents an important step for the region, it again must be pointed out that enforcement to date has been unsatisfactory. Even so, we posit that legislation represents the first step in the process of protecting women from online harassment and is a baseline for holding perpetrators accountable. We urge all countries to take that first step.

Barriers to Policy Responses: MENA and Why WhatsApp?

Barriers to policy responses are specifically prevalent in the MENA and African regions. When nations simply do not care about women’s physical security, they certainly will not care about her security online, or how online effects can lead to a dangerous physical environment. To put this in perspective, action on technology-facilitated gender-based violence has been particularly difficult in the MENA region. For example, Turkey, a NATO ally, has seen major regression in women’s rights and physical security. In 2021, Turkey pulled out of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, or the Istanbul Convention.²³⁰ Turkey’s major issues with femicide in general, and its suppression of human rights groups and NGOs, demonstrates how many of the countries in the MENA region are not, in general, overly concerned with women’s security either online or offline.²³¹ National or multilateral initiatives can only succeed in countries that are willing to value addressing these issues upfront, in the first place.

In addition to the action taken by governments, private companies, and NGOs, Saskia Brechenmacher, Fellow for Democracy Conflict & Governance at the Carnegie Endowment for International Peace, noted in our interview that some problems with online harassment are actually platform-specific. For example, there are struggles in Africa when it comes to the regulation of gender-based online harassment because one of the predominant social media platforms used in the region is WhatsApp, owned by Facebook. The private nature of the platform and the “design means WhatsApp has little control over what content takes off and what doesn’t; in most cases, the company cannot even see what is happening on WhatsApp, because the service encrypts messages automatically.”²³² In Kenya, social media influencers were being contacted via WhatsApp to promote political misinformation in exchange for money. For example, “[t]he research showed the disinformation business to be lucrative, with influencers for political hire paid roughly between \$10 (£7) and \$15 to participate in three campaigns per day. Some influencers managed to reach retainer level and were paid about \$250 per month... Those behind the campaigns used WhatsApp groups to send influencers content and detailed instructions.”²³³

Other regions have also seen problems with this particular platform. India has gone to great lengths to prevent people from being able to mass spread information on WhatsApp and has limited the number of chat groups a message can be forwarded to.²³⁴ It may be wise for Africa to follow suit in this legislation, as it may be the only path to limit the spread of harassment on that particular platform. Governments will need to consider such platform-specific idiosyncrasies when crafting legislation.

Gaps in the Research and Literature

Our efforts this semester have led us to understand that the existing research literature is not sufficient in its assessment of the relationship between gender-based online harassment and women’s political participation. First, there are few data sets available that accurately depict the frequency and type of online harassment, especially as it pertains to women. Most data are derived from surveys, and make assertions based on inadequate sample sizes for one country. If there is no baseline measurement of the online harassment of women, there is no way to determine if policy initiatives are making any difference at all. Governments are making policy

without any possible means of monitoring or evaluating its efficacy. When one turns specifically to online gender-based violence towards women in politics, while there is separate data regarding online harassment of women and that of politicians, there are distinct gaps at the intersection of the two. Data can be pulled from selected articles, however, there is no consolidated dataset to draw from even for a single country, much less globally. Much of the data to be found also focuses on the United States or the United Kingdom.

Further, there is virtually no information on the actors perpetrating the harassment. Without an understanding of who is actually committing these offenses, how can policy making be effective? Additional data needs to be collected on this front, and that will require resources that perhaps only a government or IGO could sustain over time.

Second, there is insufficient information on the differences in experiences and consequences for women who identify with specific minority groups. There is evidence of BI-POC women experiencing higher levels of online harassment but there is a lack of information on how other factors may influence this such as religion, sexuality, and political views. Intersectional identities are critical to the contextualization of, specifically, online abuse and technology-facilitated gender-based violence. In order to appropriately create effective policy, policymakers need to understand the diversity of the groups that are disproportionately impacted.

Third, bots as perpetrators of online harassment deserve higher prioritization in literature, and will need to be factored into the data collection effort we are recommending. Nora Lindström points out that 15% of all Twitter profiles are presumed to be bots. A huge gap in the literature involves the lack of studies done on bots and how they may contribute to the gender-based online harassment problem.²³⁵ While there is ample literature on bots consistently spreading misinformation regarding topics such as COVID-19, there is almost nothing in the literature on their involvement with online harassment of women and technology-facilitated gender-based violence.²³⁶ It can be assumed that misinformation, harassment, and violence against female political leaders can be perpetrated by bots, and that this can produce the same harmful effects as non-bot harassment. Lindström discusses how bots “have also attacked progressive action in Australia. A bot was found to be attempting to derail Plan International’s own Free to Be research on street harassment. We were using an online map-based tool, which young women could drop pins on to identify areas where they felt safe and unsafe. This bot had

been programmed to drop pins continuously in order to invalidate the results.”²³⁷ The lack of research into who exactly is perpetuating gender-based online harassment, bot or not, is something that needs to be addressed in order to make sustainable, suitable policy.

Fourth, there has been a complete lack of studies on AI algorithm gender bias and how this can affect opportunities for women in politics. We view AI bias as a subtle form of online harassment which may have similar effects to traditional forms of online harassment. There has been one study so far that has noted Google Search Engine gender bias for politics-specific job searches.²³⁸ This is not enough to accurately depict whether or not there are biases in these algorithms, and whether or not having more female programmers on these teams would help mitigate bias. Google is still currently under fire for having a gender bias in image searches for powerful jobs or positions.²³⁹ Another study revealed that Facebook had gender bias in its job advertisement targeting, so we can assume that this bias likely carries over to political jobs and women’s political involvement.²⁴⁰ Data needs to be collected on these algorithms and how they may possibly aggravate issues that pertain to a lack of women’s political participation--by possibly not showing them opportunities to be politically involved at all.

Fifth, in order to analyze regional trends in policy this report has utilized the Summit for Democracy’s list of member country commitments to draw out trends as they pertain to cyber legislation as well as gender equality initiatives. Although there were over 275 participants in the form of heads of state, NGOs, activists, journalists, etc., only a handful of participating countries in the Summit for Democracy supplied policy initiatives they would be taking in response to the call for preventing democratic backsliding. The lack of truly global participation leaves gaps in regions such as Latin America, Near East, and Africa.

Policy Recommendations

The challenge to democracy represented by the online harassment of women political figures is not unique to the U.S. It has and will continue to challenge the vitality and stability of democracy across the world. For this reason, the U.S. must not only take steps to combat the spread and mitigate the effects of gender-based online harassment and abuse domestically, it must also work collaboratively through international mechanisms and partnerships to actively coordinate policy approaches.

I. Executive Branch

A. Expanding Upon and Supporting Denmark's Technology for Democracy Initiative

1. This initiative would ensure countries are sharing information and policies on how they are approaching the issue. Countries need initiatives like this that provide forums for states to meet and discuss policies in order to have discussions on what has worked and what has not. Citizens also need to know what their governments are doing, and what other countries are doing. Researchers need to know what policies are in place, and which are proposed. This is low-hanging fruit, and should be effected immediately.
2. Non-democratic nations must be brought into the dialogue. A similar initiative to the Tech for Democracy Initiative, perhaps called the Tech for Good Governance Initiative, should be started that also gives non-democratic countries an invitation to join democracies in a platform to discuss these issues; maybe this general global forum might be pursued under UN auspices. Since USAID and DoS are working with developing countries, the Global Partnership can also be used to have these discussions with those countries involved as well.

B. Invest in Research - **Department of State/Department of Justice**

1. Broader Data Collection
 - a) We recommend standardized data collection, and recommend it begin immediately, spearheaded by the **Department of Justice** for prosecutorial purposes and the **Department of State** because it should be facilitating international collaboration in this policy space. This will involve standard definitions of terms, and standard categories of data to be collected by government statistical bureaus. When online harassment begins threatening a person's well-being, it is the nation's **law enforcement agencies** that should be tasked with this endeavor. Rational policy-making cannot proceed without a baseline understanding of the frequency and type of harassment faced by women as well as women politicians.

An understanding of who is actually perpetrating the abuse will also need to be part of this data collection effort. It is also important to include women in local and state-level positions, which would be especially useful to see how the presence of women in positions of lesser authority can still become targets of online outrage. We urge the creation of a working group to establish standards and tasking for this data collection effort.

- b) In addition to data collection on the offense itself, also needed is a database on what governments are doing to combat it. This includes not only the presence of laws and regulations, but also indicators on whether the laws are being enforced, and what level of funding has been appropriated for the task.
- c) As noted in the section recounting the worldwide incidence of this problem, the range of types of online harassment is wide and certain types are specific to particular regions. We recommend expanded research into the cultural differences surrounding online harassment of female politicians. It should be noted that there are differences between each country that faces this issue, and the distinct makeup of targeted harassment is unique to regions. This needs to be documented in the larger data collection effort we are proposing.

2. Invest and Encourage Non-state Actors to do Research

- a) There is no data collection without dedicated funding. National law enforcement agencies should bear the ultimate responsibility for tracking these offenses, and should receive additional funding to do so. In some cases, these agencies may need to partner with NGOs and nonprofits to collect the data needed. This may include global data collection, and a U.S. analysis of other countries' data, but this is largely dependent on the policies for data collection

formulated in the multilateral initiatives discussed in the Country Action section.

- b) Indeed, we recommend the establishment of a Civil Society Working Group of nongovernmental actors that will meet periodically with government representatives to assess and suggest lines of effort to combat these offenses.

3. Bots and Algorithms - NGOs and Non-Profit Organizations, Potential for State Department Grant

- a) More research needs to be done on bots and whether or not they are perpetuating online harassment, especially against female political leaders. This research should also be supplemented by research on AI bias in search engines or job findings. This research will have to be done by the social media entities themselves or NGOs that specialize in algorithm research.

C. Set forth a set of guiding principles for the tech sector based on the UN Guiding Principles on Business and Human rights and the OECD Guidelines on Multinational Enterprises, Sustainable Development Goals to encourage due diligence and remediation measures within tech companies (especially social media and networking sites)

1. First Core Principle: Transparency and Reporting

- a) Companies should be required to publish Annual or Bi-Annual reports of all online harassment of women, minorities, and marginalized groups not being moderated out or flagged, in line with the recommendation for the mandate on data collection by companies. The steps taken to address these problems need to be released on a publicly accessible website. The need to create such a report will catalyze efforts within companies to know precisely what the experiences of their users are, and whether those experiences are improving or not with changes in company procedures.

- b) These reports and all information must also be in plain English with numbers explained, and the company should offer multiple translations of these reports in the languages of the countries in which these tech companies operate

2. Second Core Principle: Directors' Duty of Care

- a) Corporate Responsibility defines the duty of care as the duty by which a corporate director or officer is required to perform their functions in good faith, in a manner that they reasonably believe to be in the best interests of the corporation, and with the care that an ordinarily prudent person would reasonably be expected to exercise in a like position and under similar circumstances.
- b) Corporate leaders should be held personally responsible for negligence in addressing these issues. This will create added incentive for leadership to remain dedicated and vigilant to the remediation of these issues.
- c) One possible area of negligence that can be litigated is in the area of risk assessment for products deployed in the public square. A gendered risk assessment must be mandated before such deployment.
- d) A second area of negligence that can be litigated is in the area of remediation of offenses. Litigation could inquire into the timing of the deletion of harassing material, actions taken towards perpetrators, compensation for victims, and so forth.
- e) Some have suggested that management can appoint their own Algorithm Czar or corporate eSafety commissioners who will be held responsible for not addressing these issues. This is in addition to similar positions within the government.

D. We recommend that the USG implement/State Dept advocate for a dedicated department, agency, or program that provides all necessary resources internally to USG personnel. Existing agencies alone do not have the resources or bandwidth

to adequately address this issue. This collaborative entity, with a similar framework to the National Counterterrorism Center, would ideally be composed of representatives from the Department of Justice, the Office of Management and Budget, and law enforcement bodies. It will:

1. Educate on online harassment
 2. Provide resources and protection to women who disproportionately experience online harassment. Offer a Victim's Bill of Rights that a victim can use to assert their legal rights vis a vis a tech company.
 3. Facilitate dialogue between politicians and private sector on this issue
 4. Investigate and act on potential threats to female politicians
- E. Recognizing the psychological and emotional impact of online harassment and abuse, USG agencies should employ a victims-centered and/or trauma-informed approach, like that being promoted by anti-trafficking interagency groups and participating departments, to provide resources and support for female political figures dealing with this issue. By prioritizing the mental health of politically-active women, USG agencies can foster a safe environment that permits equal access to politics. - **Law Enforcement Agencies (DHS, FBI, State and Local)**
1. See resources from Office for Victims of Crime Training and Technical Assistance Center (OVCTTAC)²⁴¹ on "Victim-Centered" and the State Department's Trauma-Informed Approach²⁴²
 - a) Politically-active women's wishes, safety, and well-being take priority
 - b) Online training modules for staff and law enforcement on how to appropriately address issues pertaining to victims of online abuse and violence - Online Training Module from OVCTTAC²⁴³
 - c) Joint relationships with counseling services and cyber-units of law enforcement
 - d) Victims Assistance Training Online Module

F. Grassroots (K-12) and General Public Education Initiatives - **Department of Education**

1. Digital Literacy Education: Social media is not going anywhere. If anything, its accessibility and complexity will continue to increase. Children are receiving phones and tablets at younger ages than ever before. Depending on the parenting style, some children will have unrestricted access to the internet and social media platforms. With the normalization of elementary-aged children having access to technological devices, it is imperative that children, from K-12, achieve digital literacy. Encouraging digital literacy education is a proactive measure that would help reduce the number of online harassment perpetrators. According to the American Literacy Association, digital literacy is “the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills”.²⁴⁵ Proper digital literacy education through a grassroots (K-12) program, mandated by Department of Education standards, would provide children with the skills needed to navigate technology safely and beneficially. Instilling knowledge about the internet and social media etiquette could steer individuals away from harassing others later in life. With this early start approach, future generations of female political figures may be able to work in an environment that has appropriate online etiquette.

G. Government and Private Sector Partnerships - **Office of Management and Budget, Department of Commerce**

1. Use collaborative working groups to bridge the gap between the tech sector and the executive branch. For example, using AI technologies to fight against malicious bots could be one strong point of collaboration for tech companies and the government, with the aim of more effectively using moderating technology to stop online harassment of women. This partnership could also be an effective approach for the government to gain some headway on mitigating unsafe online behavior against women by

preemptively encouraging companies to act on this issue before legislative measures are enacted. Working groups have seen extensive success in the cybersecurity field and by utilizing similar frameworks as working groups such as the Conficker Working Group, a collaborative coalition of cybersecurity professionals in the private sector, academia, and law enforcement made in response to the outbreak of a botnet attack. This can be mimicked to help fight online harassment of women.

H. Facilitate the Creation of eSafety Commissioner Programs for Countries

1. The eSafety Commissioner programs should be part of the Global Partnership and should have one focus area in line with gender-specific online harassment and the online harassment of women in politics. This way the program will specifically address this issue, and the online harassment of women is outlined as an important priority upon the program's implementation. These programs will be modeled on the Australian program mentioned in the Country Action section of the paper.
2. eSafety commissioners could act as the head of an administrative agency that oversees the interagency process as outlined (See the DHS Interagency Security Committee²⁴⁶ or the White House Interagency Task Force to Monitor and Combat Trafficking in Persons²⁴⁷ as an Organizational Template)
3. eSafety Commissioners would mandate companies track data regarding frequency of online harassment and abuse, profiles of perpetrators, number of victims and associated risk factors that may increase their likelihood of harassment. This would grant eSafety Commissioners some form of regulatory or statutory authority.
4. Similar to the all-female police units in India that predominantly deal with women's reports of domestic violence, all-female police units should be created to enforce online harassment and technology-facilitated gender-based violence laws (or women's physical security laws) in the U.S. and countries where cultural norms against women permit these laws to go unenforced.

- a) A dedicated law enforcement unit is needed so current police forces are not further back-logged, these units should span from local to federal levels. Additional funding to police forces has not proved successful in alleviating current work loads thus far, so a separate, dedicated unit is necessary. For example, currently, police forces have hundreds of thousands of untested rape kits around the country.²⁴⁸ In order to not add to the existing strain on their time and resources, we propose a dedicated unit at the federal and local level. Funding should be allocated to these units specifically

I. Multilateral Initiatives/Policies

- 1. Use the framework of the Global Internet Forum to Counter Terrorism (GIFCT) as a baseline for technology companies to create a similar NGO organization that addresses instances of online harassment and TFGBV.
 - a) The Global Internet Forum to Counter Terrorism has a database sharing system that tracks instances of terrorism and media uploaded by terrorist organizations, then inserts these instances into an international database. This helped tech organizations consolidate definitions of “terrorism” and “terrorist content”.²⁴⁹ The goal of this was to prevent terrorist organizations from exploiting their platforms. This is the most useful part of the GIFCT framework- a similar, multinational, multi-tech organization, program can be created to track instances of online harassment and TFGBV. This can also help tech companies consolidate definitions. The biggest use in this is how GIFCT was able to create a database that tracked whether or not online terrorist activity translated to the physical world through acts of violence. The GIFCT is an NGO founded by Facebook, Microsoft, Twitter, and Youtube in 2017 to “foster technical collaboration among member companies, advance relevant research, and share knowledge with smaller platforms... and counter the spread of terrorist and violent extremism content online”.²⁵⁰ This framework can also be

used to counter the spread of gendered misinformation and track data on online harassment and TFGBV occurrences through a similar set of private social media companies.

2. Use international framework laws such as those for money laundering and trafficking as a baseline for fostering international action and policy on TFGBV and online harassment, especially as they relate to female politicians and democracy. This could possibly be facilitated by the UN and include other global NGOs. - **Department of State/US Rep to UN**

- a) International action against money laundering uses several initiatives to emphasize consolidation of policy, and put all countries on the same page in terms of money laundering and consequences associated with it. International organizations attempt to promote accountability with those countries that have prominent money laundering issues, or for those countries that do not address the issues at all.

- (1) An international task force was created to address the issue, the Financial Action Task Force. It currently issues recommendations for states on approaching money laundering.²⁵¹ This promotes a sense of consolidation in action. This is another international framework that can be adopted for multilateral efforts on TFGBV and online harassment of women. An international task force would be a great start for multilateral efforts. The FATF currently has member countries from the Middle East and Africa, so a framework similar to this may be the best way to bring these countries into the conversation initially.

- (2) “Naming and shaming”- States should be “named and shamed” by the UN if they are non-compliant with UN international standards on violence against women, specified in the Convention on the Elimination of All

Forms of Discrimination Against Women, especially if they have ratified it. Examining action against online harassment of women political figures should be made part of the CEDAW Commissions' remit when it writes its Concluding Observations on submitted country reports.

- (3) Member states that want to influence financial intelligence efforts must remain compliant with international organization standards.²⁵² Member states that want to reap the benefits of efforts against these crimes, need to abide by an international framework that sets the stage for addressing TFGBV as a crime and a threat to democracy. If states have some sort of stake in the game when it comes to intelligence on the democratic effects of TFGBV and online harassment of women, they may be more likely to uphold the international standards and policies created on it.

3. Include clauses in regional trade agreements that incorporate protection and liability mechanisms for technology companies who fail to remediate issues concerning online harassment of female political figures on their respective platforms. - **U.S. Trade Representative**

- a) Trade agreements are uniquely positioned to establish legal obligations for the enforcement of human rights and sector-specific issues. The Biden Administration's 2022 Trade Agenda²⁵³ aims to insulate sustainable environmental practices in trade agreements, the success of which will be seen in the coming years. Meanwhile, the 2020 U.S.-Mexico-Canada²⁵⁴ trade agreement's labor clauses have contributed to Mexico's adoption of better labor practices and standards, especially in terms of union support. Once the U.S. has appropriate policies on the space of online harassment and abuse and tech sector responsibility, it can take steps to engrain them in

trade agreements with partner countries and encourage them to do the same.

4. We strongly encourage the US Congress to ratify the Convention on the Elimination of all forms of Discrimination Against Women (CEDAW) to provide an international legal framework for US women's rights.

J. Development/Foreign Assistance - **USAID, Department of State, Department of Labor, Department of Defense (Sub-Agencies)**. The Biden Administration has proposed \$2.6 billion for the purposes of advancing gender equity and equality in FY 2023 to be spent through foreign assistance.^{[255](#)}

1. Security-Sector Focused

- a) Similar to how the State Department's Bureau of International Narcotics and Law Enforcement Affairs works to keep Americans safe by countering crime, illegal drugs, and instability abroad through INL's work with partner nations, this can also extend to the prosecution of online harassment. By utilizing the Bureau's engagement with the entire spectrum of criminal justice systems among partner nations, including law enforcement, judges, prosecutors, defense attorneys, and correctional institutions with partner nations, the US can help other countries begin to prioritize the prosecution of online harassment internationally.
- b) Similar to the all-female police units in India that predominantly deal with women's reports of domestic violence, all-female police units should be at the forefront of enforcing online harassment and technology-facilitated gender-based violence laws in the U.S. and countries (or women's physical security laws) where cultural norms against women permit these laws to go unenforced. These units should span the federal to local level, especially as the local level will likely have to enforce cyberstalking/cyberharassment laws.

(1) We also recommend the implementation of all-female enforcement units to uphold women's physical security laws, especially in regions where cultural norms against women are strong.

c) It is also recommended that women who experience serious online threats have access to a direct reporting system to law enforcement. This would also allow law enforcement to collect data on frequency of attacks.

2. The Advancing Women's and Girls' Civic and Political Leadership Initiative, as discussed in the Country Action section, should be built upon and needs to actually act on the commitments they outlined. **USAID and DOS**

a) "USAID will expand its digital programming in support of open, secure, and inclusive digital ecosystems that advance democracy, counter digital authoritarianism, promote digital literacy and provide equitable access to underserved communities."²⁵⁶

b) USAID and DOS need to set concrete objectives and plans of action in line with our recommendations and in consultation with the Civil Society Working Group.

K. Private Sector Investment Programming

1. Another way to combat online harassment of women in politics is for governments to subsidize or invest in private companies that clean up harmful bots, monitor and track online harassment data, and create bots that balance the harassment with positivity. Companies like ParityBot, Areto Ally, and Moonshot do this work but only for paying clients. These companies are small but have the potential to expand their work given adequate funding.

II. Legislative Branch

A. Educating Congress on Online Harassment and Abuse

1. Ask specific Congressional committees to hold special hearings on this topic so that legislation will be informed by knowledge. For example, it may be necessary to demonstrate that there is a difference in what men experience versus what women experience, especially those involved in the political space. Congress needs to be educated on the issue before it can pass laws on the subject.
2. Currently, all members of Congress must take a course on sexual harassment. Online harassment could be an addition to the existing course.

B. Pass the following laws:

1. H.R.2154 - Protecting Americans from Dangerous Algorithms Act which would remove large tech platforms' legal immunity for violent or violence-inciting content that their feed-ranking and recommendation systems amplified, while preserving their immunity for other user-generated content.^{[257](#)}
2. S.1896 - Algorithmic Justice and Online Platform Transparency Act / H.R.3611 - Algorithmic Justice and Online Platform Transparency Act that "establishes requirements for certain commercial online platforms (e.g., social media sites) that withhold or promote content through algorithms and related computational processes that use personal information."^{[258](#)}

III. Private Sector Initiatives

A. Companies

1. Incentivize tech companies to bring women, minorities, and locals into the company to bring insight and understanding on how to address marginalization that is perpetuated in online fora - **FCC, Dept of Commerce?**
 - a) Tech companies can greatly benefit by recruiting women and minorities onto programming and moderation staff. There is a real need for more women coders to program AI moderation because women are first-hand witnesses and victims of specific abuse.

Women and minorities need to be prioritized in programming positions because there is a current lack of intersectional expertise in content moderation, which results in abuse of women, minorities, and people of color falling under the radar. There also needs to be women writing social media platform policies. Most platform policies lack a methodical definition of online harassment/abuse, meaning that the abuse women face online does not violate any policies or guidelines. Perpetrators are therefore able to continue their abuse without fear of being moderated out or punished.

- b) Another issue facing tech company success in content moderation is the lack of local moderators employed by these companies. In many cases, only local moderators can understand the context, meaning, and intent of online abuse. As discussed throughout the paper, online harassment of women looks different in every country. Something that may be offensive in Bangladesh may not be seen as offensive in the United States. Money needs to be allocated to the employment of local moderators, especially during elections.

2. Social Media/Tech Companies: Government Initiatives to Hold Tech Companies Accountable

a) Algorithmic Accountability

- (1) Since online harassment is becoming criminalized, we urge the DoJ to mandate that companies provide their algorithm programmers with top of the line training on the evolving nature of threats online, specifically those aimed at women in politics. Companies must certify such training is taking place, and indicate how their algorithms have changed to address these issues.

b) Moderation Accountability

- (1) It is becoming increasingly obvious that the government must set standards for moderation of online content. It should no longer be the case, for example, that tech companies can treat sex-based harassment as trivial compared to harassment of other groups. The U.S. government must provide these guidelines so that negligence can be litigated in courts of law.
 - (a) There is opportunity for the Securities and Exchange Commission to assist in reinforcing guidelines on moderation through the creation of rules which would require public companies to assess business operations and publicly disclose their findings.
- (2) We note as a tangent that tech companies who employ content moderators to flag abusive content need to take concrete steps to better care for moderators. Moderators are often overworked and deal with traumatic content all day. Social media and tech companies need to hire many more moderators to help lighten the load of the job. Additionally, moderators should be making a living wage, have access to employee benefits, and should be provided with counseling services during their work week to help work through the violence they moderate.
- (3) We recommend the creation of all-female moderation units for the major social media platforms. These teams would be tasked with moderating harassment and incidents of technology-facilitated gender-based violence.
- (4) Tech and social media companies can adopt strategies like the one at Moonshot. Moonshot “identifies, maps, and provides critical analysis on online harms across the globe

and offers the most advanced online interventions available today. Rooted in evidence, Moonshot disrupts malicious actors, counter their messages, and provide services to steer people away from violence. We work with established local support services and intervention partners, including trained counselors, mentors, and community leaders.” Companies can partner with organizations like Moonshot to develop algorithms to effectively counter online abuse

B. Stakeholders and Investors

1. Investor Side: There is a space for the U.S. to work with investors, stakeholders, other actors in the finance sector to ensure enforcement or incentivize compliance with tech regulations. Leverage the money for change.
 - a) Merger and Acquisition due diligence is increasingly concerned with risks and GDPR compliance of tech companies/tech departments within companies²⁵⁹
 - b) The NAP on Human Trafficking released by the Biden Administration in December 2021 - focusing on supply chains and the issue of forced labor, implements strategies to engage and educate relevant private sector partners. The trafficking NAP includes educational programs, and highlights existing federal resources which seek to engage with investors on these issues to ensure they are aware of the supply chain risks associated with forced labor and human trafficking. This can translate to those who hold equity in technology companies fairly easily, in that investors should be made aware of the behavior and actions that are facilitated on specific social media platforms or through telecommunication devices. There should be “[p]roactive outreach to convene industry leaders” and through this outreach the

“[inclusion of] presentations and webinars,...facilitated discussions,...general info sessions[,] and deeper discussions for challenges [and] opportunities”²⁶⁰ within the space.

Conclusion

The presence of online harassment and abuse is a global threat to women, undermining both their political voice and their democratic participation. Without addressing this issue, democracies facilitate the dissolution of liberal principles throughout the whole of government. The serious threats that female politicians face online and in their everyday lives sets a precedent for women everywhere. If you open your mouth, you will be raped, beaten, or killed. Since the violence and misogyny has inevitably seeped into the technological realm, action must be taken to address this issue. If we are to combat the proliferation of this issue, we must learn more, collect more data, facilitate stronger programs and legislation, and educate our policymakers and people as a nation. We need to hold technology companies accountable and substantiate our lines of effort to a standard that allows for tangible results. Choosing not to remediate this issue by any means would be a detriment to democracy.

Bibliography

- Abdul-Hassan, Ali and Salaheddin, Sinan. (2018). Despite Challenges, Iraq's Female Candidates Run for Parliament. *Christian Science Monitor*. Retrieved from <https://www.csmonitor.com/World/Middle-East/2018/0503/Despite-challenges-Iraq-s-female-candidates-run-for-parliament>
- Al Jazeera. (2018). Morocco criminalises violence against women and sexual harassment. *Women's Rights News | Al Jazeera*. Retrieved from <https://www.aljazeera.com/news/2018/9/12/morocco-criminalises-violence-against-women-and-sexual-harassment>
- Amnesty International (2020). Troll patrol findings. *Troll Patrol Report*. Retrieved from <https://decoders.amnesty.org/projects/troll-patrol/findings>
- Areto Labs. (n.d.). Retrieved from <https://www.aretolabs.com/>
- Astor, M. (2018). For Female Candidates, Harassment and Threats Come Every Day. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/08/24/us/politics/women-harassment-elections.html>
- Australian Government. (n.d.). About the commissioner | Esafety commissioner. *eSafety Commissioner*. Retrieved from <https://www.esafety.gov.au/about-us/who-we-are/about-the-commissioner>
- Australian Government. (n.d.). Our legislative functions. *eSafety Commissioner*. Retrieved from <https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>
- Atalanta (2018). (Anti) Social Media: The Benefits and Pitfalls of Digital for Female Politicians. Retrieved from <https://www.atalanta.co/news/2018/3/13/antisocial-media-the-benefits-and-pitfalls-of-digital-for-female-politicians>
- Axline, A. (2022). Areto Labs: Using technology to combat online toxicity. *About Alberta Tech*. Retrieved from https://www.aboutalbertatech.com/post/areto-labs-using-technology-to-combat-online-toxicity?utm_source=hs_email&utm_medium=email&hsenc=p2ANqtz-SLI5y7FTZWWAUiiNZK6oQFnZEB-KreAOYVQGhOOEdGPuTlaPYO-N_PdpVNQw6T9a2FdW
- Barker, K., & Jurasz, O. (2021). Text-based (sexual) abuse and online violence against women: Toward law reform? *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 247–264. Retrieved from <https://doi.org/10.1108/978-1-83982-848-520211017>
- Biden Campaign. (2020). Joe Biden's plan to end violence against women. *Joe Biden for President: Official Campaign Website*. Retrieved from <https://joebiden.com/vawa/>
- Big Brother Watch. (2021). The State of Free Speech Online. *Big Brother Watch: Defending*

- Civil Liberties, Protecting Privacy*. Retrieved from <https://bigbrotherwatch.org.uk/wp-content/uploads/2021/09/The-State-of-Free-Speech-Online-1.pdf>
- Blume, L. R. (2017). The old rules no longer apply: Explaining narco-assassinations of Mexican politicians. *Journal of Politics in Latin America*, 9(1), 59–90. Retrieved from <https://doi.org/10.1177/1866802x1700900103>
- Brechenmacher, S., & Di Meco, S. (2020). Tackling Online Abuse and Disinformation Targeting Women in Politics. *Carnegie Endowment for International Peace*. Retrieved from <https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331>
- Brechenmacher, S., & Mann, K. (2022). Renewing U.S. investments in women's political leadership. *Just Security*. Retrieved from <https://www.justsecurity.org/79992/renewing-u-s-investments-in-womens-political-leadership/>
- Bridoux, J., & Kurki, M. (2014). *Democracy promotion: a critical introduction*. Routledge.
- Bureau of International Labor Affairs. (2022). Labor Rights and the United States-Mexico-Canada Agreement (USMCA). Retrieved from <https://www.dol.gov/agencies/ilab/our-work/trade/labor-rights-usmca>
- Carry, G. (2019) At the GDPR's First Anniversary, the Impact on US Companies Grows. *Data Law Insights*, Retrieved from <https://www.crowelldatalaw.com/2019/06/at-the-gdprs-first-anniversary-the-impact-on-us-companies-grows/>.
- Chenoweth, E., & Zoe Marks. (2022). Revenge of the Patriarchs: Why Autocrats Fear Women. *Foreign Affairs*. Retrieved from <https://www.foreignaffairs.com/articles/china/2022-02-08/women-rights-revenge-patriarchs>
- Clinton, H. R. (1999). Remarks and commentary by first lady Hillary Rodham Clinton--vital voices, 1997-1999. Executive Office of the President.
- Clontz, C. (2020). Violence against women in politics in Bolivia. *Panoramas*. Retrieved from <https://www.panoramas.pitt.edu/news-and-politics/violence-against-women-politics-bolivia>
- Crockett, C. & Vogelstein, R. (2022). Launching the Global Partnership for Action on Gender-Based Online Harassment and Abuse. *The White House Gender Policy Council*. Retrieved from <https://www.whitehouse.gov/gpc/briefing-room/2022/03/18/launching-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/>

- Duggan, M. (2017). Americans' online harassment experiences. *Pew Research Center: Internet, Science & Tech*. Retrieved from <https://www.pewresearch.org/internet/2017/07/11/experiencing-online-harassment/>
- Ejaz, B., & Imtiaz, S. (2015). Sexual harassment: A study of mal-adaptation of information and communication technology. *The Explorer: Journal of Social Sciences*, 1(3), 58-61. Retrieved from https://www.academia.edu/11723046/SEXUAL_HARASSMENT_A_STUDY_OF_MAL_ADAPTATION_OF_INFORMATION_AND_COMMUNICATION_TECNOLOGY
- General Data Protection Regulation (GDPR). (2018). *General Data Protection Regulation (GDPR)* Retrieved from <https://gdpr-info.eu>
- GIFCT. (2022). What we do: Tech innovation. *GIFCT*. Retrieved from <https://gifct.org/tech-innovation/>
- GIFCT. (2022). Who we are: About. *GIFCT*. Retrieved from <https://gifct.org/about/>
- GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Retrieved from <https://gbvaor.net/index.php/node/1155>
- Hassan, F. M., Khalifa, F. N., El Desouky, E. D., Salem, M. R., & Ali, M. M. (2020). Cyber violence pattern and related factors: online survey of females in Egypt. *Egyptian journal of forensic sciences*, 10(1), 1-7. Retrieved from <https://doi.org/10.1186/s41935-020-0180-0>
- Harmer, E., & Southern, R. (2021). Digital microaggressions and everyday othering: An analysis of tweets sent to women members of Parliament in the UK. *Information, Communication & Society*, 24(14), 1998–2015. Retrieved from <https://doi.org/10.1080/1369118X.2021.1962941>
- Heilweil, R. (2020). Why Algorithms Can Be Racist and Sexist. *Vox*. Retrieved from <https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparenc>
- Himelein-Wachowiak, M., Giorgi, S., Devoto, A., Rahman, M., Ungar, L., Schwartz, H.A., Epstein, D. H., Leggio, L., & Curtis, B. (2021). Bots and Misinformation Spread on Social Media: Implications for COVID-19. *Journal of medical Internet research*, 23(5). Retrieved from <https://doi.org/10.2196/26933>
- Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2022). Technology-Facilitated GBV: What is it, and How Do We Measure It?. *ICRW*. Retrieved from <https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/>

- Horwitz, J. (2021). Facebook algorithm shows gender bias in job ads, study finds. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/facebook-shows-men-and-women-different-job-ads-study-finds-11617969600>
- House of Representatives, H. R. 2154 (2021). Congress.
- Human Rights Watch. (2022). Turkey defies international human rights law. *Human Rights Watch*. Retrieved from <https://www.hrw.org/news/2022/01/13/turkey-defies-international-human-rights-law#>
- Hunt, E., Evershed, N., Liu, R. (2016). From Julia Gillard to Hillary Clinton: Online abuse of politicians around the world. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/datablog/ng-interactive/2016/jun/27/from-julia-gillard-to-hillary-clinton-online-abuse-of-politicians-around-the-world>
- IBM Cloud Education (2020). Artificial Intelligence (AI). IBM. Retrieved from <https://www.ibm.com/cloud/learn/What-is-artificial-intelligence>
- Interagency Security Committee. (2013). The risk management process for federal facilities. *CISA*. Retrieved from <https://www.cisa.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf>
- International Foundation for Electoral Systems. (2021). Assessment of Online Violence Against Politically and Civically Engaged Women in Bangladesh. *International Foundation for Electoral Systems*. Retrieved from <https://www.ifes.org/publications/assessment-online-violence-against-politically-and-civically-engaged-women-bangladesh>
- Inter-Parliamentary Union. (2018). Sexism, harassment and violence against women parliamentarians. *Council of Europe*. Retrieved from https://doi.org/10.1163/2210-7975_HRD-1021-2016006
- Iyer, B. Nyamwire & S. Nabulega (2020). Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet. *Pollicy*. Retrieved from <https://ogbv.pollicy.org/report.pdf>
- Jane, E. A. (2016). *Misogyny online : A short (and brutish) history*. SAGE Publications.
- Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S., & Kaufman, Z. (2021). Malign Creativity - Wilson Center. *Wilson Center*. Retrieved from https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Report%20Malign%20Creativity%20How%20Gender%2C%20Sex%2C%20and%20Lies%20are%20Weaponized%20Against%20Women%20Online_0.pdf

- Kakande, A., Achieng, G., Iyer, N., Nyamwire, B., Nabulega, S., & Mwendwa, I. (2021). Amplified Abuse: Report on Online Violence Against Women in the 2021 Uganda General Election. *Pollicy*. Retrieved from <https://archive.pollicy.org/wp-content/uploads/2021/08/Amplified-Abuse-Report.pdf>
- Karakas, B. (2020). Turkey: Laws against domestic abuse fail to protect women. *DW.COM*. Retrieved from <https://www.dw.com/en/turkey-laws-against-domestic-abuse-fail-to-protect-women/a-55717911>
- Keating, J. (2009). Orthodox Paper Photoshops Women Out of Israeli Cabinet. *Foreign Policy*. Retrieved from <https://foreignpolicy.com/2009/04/03/orthodox-paper-photoshops-women-out-of-israeli-cabinet/>
- Kishi, R. (2021). Violence Targeting Women in Politics: Trends in Targets, Types, and Perpetrators of Political Violence. *ACLEDD*. Retrieved from <https://acleddata.com/2021/12/08/violence-targeting-women-in-politics-trends-in-targets-types-and-perpetrators-of-political-violence/>
- Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755. Retrieved from <https://doi.org/10.1017/S1537592719001397>
- Kwan, C. (2022). E-safety outlines long list of challenges within Australia's proposed anti-trolling laws. *ZDNet*. Retrieved from <https://www.zdnet.com/article/esafety-outlines-long-list-of-challenges-within-australias-proposed-anti-trolling-law/>
- Lamensch, M. (2021). When Women Are Silenced Online, Democracy Suffers. *Centre for International Governance Innovation*. Retrieved from <https://www.cigionline.org/articles/when-women-are-silenced-online-democracy-suffers/>
- Levitsky, S. & Ziblatt, D. (2019) *How Democracies Die*. Broadway Books.
- Lilleker, D., Koc-Michalska, K., & Bimber, B. (2021). Women learn while men talk?: Revisiting gender differences in political engagement in online environments. *Information, Communication & Society*, 24(14), 2037–2053. Retrieved from <https://doi.org/10.1080/1369118X.2021.1961005>
- Lindström, N. (2019). Think you're being abused by a sexist troll? It could be a bot. *New Matilda*. Retrieved from <https://newmatilda.com/2019/05/02/think-youre-being-abused-by-a-sexist-troll-it-could-be-a-bot/>
- Manjoo, F. (2018). The problem with fixing WhatsApp? Human nature might get in the way. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/10/24/technology/fixing-whatsapp-disinformation-human-nature.html>

- McGreal, C. (2012.) Arab Women Fights to Keep Gains Won on the Street. *The Guardian*. Retrieved from <http://www.guardian.co.uk/world/2012/jun/13/arab-women-egypt-laws-parliament>
- Mchangama, J., & Fiss, J. (2019). Germany's online crackdowns inspire the world's dictators. *Foreign Policy*. Retrieved from <https://foreignpolicy.com/2019/11/06/germany-online-crackdowns-inspired-the-worlds-dictators-russia-venezuela-india/>
- McQuate, S. (2022). Google's 'CEO' image search gender bias hasn't really been fixed. *UW News*. Retrieved from <https://www.washington.edu/news/2022/02/16/googles-ceo-image-search-gender-bias-hasnt-really-been-fixed/>
- Mendoza, C., & Zurka, K. (2022). The summit for democracy: Advancing gender equity and equality for Representative Societies . *United States Department of State*. Washington, DC: U.S. Department of State. Retrieved from <https://www.state.gov/dipnote-u-s-department-of-state-official-blog/the-summit-for-democracy-advancing-gender-equity-and-equality-for-representative-societies/>
- Matfess, H., Kishi, R., & Berry, M. E. (2022). No safety in numbers: Political representation and political violence targeting women in Kenya. *International Feminist Journal of Politics*, 1–23. Retrieved from <https://doi.org/10.1080/14616742.2022.2045618>
- Ministry of Foreign Affairs of Denmark. (2021). The Tech for Democracy initiative. *UM*. Retrieved from <https://um.dk/en/foreign-policy/tech-for-democracy-2021>
- National Democratic Institute. (2019). No Party to Violence: Analyzing Violence Against Women in Political Parties: Compendium Report of Country Pilots in Cote d'Ivoire, Honduras, Tanzania, and Tunisia. Washington, DC. Retrieved from http://mlkrook.org/pdf/VAW-PP_2019.pdf
- Nadim, M., & Fladmoe, A. (2019). Silencing women? gender and online harassment. *Social Science Computer Review*, 39(2), 245–258. Retrieved from <https://doi.org/10.1177%2F0894439319865518>
- National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC. Retrieved from <https://www.ndi.org/publications/notthecost-stopping-violence-against-women-politics-renewed-call-action>
- Norton, J. (2022). Online safety bill will force web giants to protect users from fraud and hate crimes. *Daily Mail Online*. Retrieved from <https://www.dailymail.co.uk/news/article-10478581/Online-Safety-Bill-force-web-giants-protect-users-fraud-hate-crimes.html>

- OAS. (2018). Anti-money laundering. *CICAD*. Retrieved from https://www.cicad.oas.org/Main/Template.asp?File=%2Fflavado_activos%2Fframework_eng.asp
- Office of Press Relations. (2021). USAID announces initiatives to advance democracy in support of Presidential Initiative for Democratic Renewal: Press Release. *U.S. Agency for International Development*. Retrieved from <https://www.usaid.gov/news-information/press-releases/dec-9-2021-usaid-announces-initiatives-advance-democracy-support-presidential>
- Office of the Spokesperson. (2022). 2022 roadmap for the global partnership for action on gender-based online harassment and abuse. *U.S. Department of State*. Retrieved from <https://www.state.gov/2022-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/>
- Office of the United States Trade Representative (USTR). (2022). 2022 Trade Policy Agenda & 2021 Annual Report. Retrieved from https://ustr.gov/sites/default/files/2022%20Trade%20Policy%20Agenda%20and%202021%20Annual%20Report_0.pdf
- Onyango, E. (2021). Kenyan influencers paid to take 'guerrilla warfare' online. *BBC News*. Retrieved from <https://www.bbc.com/news/world-africa-58474936>
- Project Someone. (2019). Online Misogyny in Canadian Politics. Retrieved from https://projectsomeone.ca/wp-content/uploads/2019/06/ONLINE-MISOGYNY_Feb2019.pdf
- Rabson, M. (2019). Threats, abuse move from online to Real World, McKenna now requires security. *CTVNews*. Retrieved from <https://www.ctvnews.ca/politics/threats-abuse-move-from-online-to-real-world-mckenna-now-requires-security-1.4582441>
- Ramalingam, V., & Frenett, R. (2022). Our Approach. *Moonshot*. Retrieved from <https://moonshotteam.com/>
- Reich, R. (2021). What Happens When a Congressman Threatens a Colleague With Violence. *The Guardian*. Retrieved from <https://www.theguardian.com/commentisfree/2021/nov/16/alexandria-ocasio-cortez-congressman-threatens-violence>
- Renaissance. (2019). What is Digital Literacy and why does it matter? *Renaissance Blog*. Retrieved from <https://www.renaissance.com/2019/02/08/blog-digital-literacy-why-does-it-matter/#:~:text=The%20American%20Library%20Association%20>
- Resnick, B. (2019). Yes, Artificial Intelligence Can Be Racist. *Vox*. Retrieved from <https://www.vox.com/science-and-health/2019/1/23/18194717/alexandria-ocasio-cortez-a-i-bias>

- Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*. Retrieved from <https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-Making%20All%20Spaces%20Safe.pdf>
- Senate and House of Representatives, S.1896, H.R.3611 (2021).
- Sobieraj, S. (2017). Bitch, Slut, skank, Cunt: Patterned resistance to women's visibility in Digital Publics. *Information, Communication & Society*, 21(11), 1700–1714. Retrieved from <https://doi.org/10.1080/1369118x.2017.1348535>
- Sobieraj, S. (2020). *Credible Threat: Attacks against Women Online and the Future of Democracy*. Oxford University Press.
- Specia, M. (2019). Threats and Abuse Prompt Female Lawmakers to Leave U.K. Parliament. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/11/01/world/europe/women-parliament-abuse.html>
- Squires, C. (2022). US cities are increasing funding for police, with Biden's blessing. *Quartz*. Retrieved from <https://qz.com/2116614/biden-calls-for-more-funding-for-police-in-us-cities/>
- State Department. (2018). Implementing a trauma-informed approach. Retrieved from <https://www.state.gov/wp-content/uploads/2019/02/283795.pdf>
- Stinson, M., & Gladstone, N. (2019). Community voices: Mobilizing for women's rights in North Africa. *RightsCon Summit Series*. Retrieved from <https://www.rightscon.org/mobilizing-for-womens-rights-in-north-africa/>
- Tcheng, H. (2020). Tech due diligence: The new pillar of M&A activity. *BearingPoint USA*. Retrieved from <http://www.bearingpoint.com/en-us/our-success/insights/tech-due-diligence-the-new-pillar-of-ma-activity/>
- Technical Division, UNFPA. (2021). Making all spaces safe. *UNFPA*. Retrieved from <https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-Making%20All%20Spaces%20Safe.pdf>
- Tenove, C., & Tworek, H. (2021). Stopping the hostile online attacks hurled at candidates. *Policy Options*. Retrieved from <https://policyoptions.irpp.org/magazines/septembe-2021/stopping-the-hostile-online-attacks-hurled-at-candidates/>
- Terry, K. (2022). Tory MP Maria Miller tells how she was cyber-flashed while on busy train into Waterloo. *Daily Mail Online*. Retrieved from <https://www.dailymail.co.uk/news/article-10656987/Tory-MP-Maria-Miller-tells-cyber-flashed-busy-train-Waterloo.html>

- The Economist Intelligence Unit. (2021). Measuring the prevalence of online violence against women. Retrieved from <https://onlineviolencewomen.eiu.com/>
- The Office for Victims of Crime Training and Technical Assistance Center. (2022). Human trafficking task force e-guide. *OVC TTAC: Office for Victims of Crime Training & Technical Assistance Center*. Retrieved from <https://www.ovcttac.gov/taskforceguide/eguide/1-understanding-human-trafficking/13-victim-centered-approach/#:~:text=Key%20Term%3A%20The%20Victim%2DCentered,se rvices%20in%20a%20nonjudgmental%20manner>
- The United States Government. (2021). Summit for democracy summary of proceedings. Washington, DC: The White House. Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/23/summit-for-democracy-summary-of-proceedings/>
- Tumulty, K., Woodsome, K., & Peçanha, S. (2020). Opinion | how sexist, racist attacks on Kamala Harris have spread online - a case study. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/opinions/2020/10/07/kamala-harris-sexist-racist-attacks-spread-online/?arc404=true>
- The United States Government. (2022). Fact sheet: Biden-Harris Administration celebrates first anniversary of the establishment of the White House Gender Policy Council. *The White House*. Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/08/fact-sheet-biden-harris-administration-celebrates-first-anniversary-of-the-establishment-of-the-white-house-gender-policy-council/>
- United Nations General Assembly. (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. Dubravka Šimonović. Retrieved from <https://digitallibrary.un.org/record/1641160?ln=en#record-files-collapse-header>
- U.S. Department of State. (2021). Unifying Trauma-Informed Practices and Voices of Survivor Leadership. *U.S. Department of State*. Retrieved from <https://www.state.gov/unifying-trauma-informed-practices-and-voices-of-survivor-leadership/>
- The United States Government. (2022). Fact sheet: President's Interagency Task Force to Monitor and combat trafficking in persons. *The White House*. Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/25/fact-sheet-presidents-interagency-task-force-to-monitor-and-combat-trafficking-in-persons/>
- United States Government. (2021). The National Action Plan to Combat Human Trafficking. *White House*. Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2021/12/National-Action-Plan-to-Combat-Human-Trafficking.pdf>

- Vagianos, Alanna. (2019). The Rape Kit Backlog Shows Exactly How We Regard Women In This Country. *Huffpost*. Retrieved from https://www.huffpost.com/entry/the-rape-kit-backlog-shows-exactly-how-we-regard-women-in-this-country_n_5acfb5e1e4b016a07e9a8c65
- Wagner, A. (2020). Tolerating the trolls? gendered perceptions of online harassment of politicians in Canada. *Feminist Media Studies*, 1–16. Retrieved from <https://doi.org/10.1080/14680777.2020.1749691>
- Wijnhoven, F., & van Haren, J. (2021). Search engine gender bias. *Frontiers*. Retrieved from <https://www.frontiersin.org/articles/10.3389/fdata.2021.622106/full>
- Winkelman, Sloane, Jody Oomen-Early, Ashley D. Walker, Lawrence Chu, Alice Yick-Flanagan. 2015. "Exploring Cyber Harassment among Women Who Use Social Media." *Universal Journal of Public Health*, 3 (5): 194-201. doi: 10.13189/ujph.2015.030504. Retrieved from <https://digitalcommons.georgiasouthern.edu/commhealth-facpubs/130>
- Yasir, S. (2022). Online ‘Auction’ Is Latest Attack on Muslim Women in India. *The New York Times*. Retrieved from <https://www.nytimes.com/2022/01/03/world/asia/india-auction-muslim-women.html>
- Pelton, M., & Songy, M. (2022, February 10). “Interview with Saskia Brechenmacher.”
- Pelton, M., & Songy, M. (2022, February 11). “Interview with Julie Denham and Caroline Hubbard.”
- Pelton, M., & Songy, M. (2022, March 1) “Interview with Josefina Erikson and Cecilia Joseffson.”
- Pelton, M., & Songy, M. (2022, February 23). “Interview with Nina Jankowicz.”
- Pelton, M., & Songy, M. (2022, March 8). “Interview with Sarah Sobieraj.”
- Pelton, M., & Songy, M. (2022, February 28). “Interview with Lucina di Meco.”

Endnotes

1. Duggan, M. (2017). Americans' online harassment experiences. *Pew Research Center: Internet, Science & Tech.*
2. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence.
3. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. Technical Division, UNFPA.
4. Sobieraj, Sarah. (2020). *Credible Threat: Attacks against Women Online and the Future of Democracy.* Oxford University Press.
5. Tenove, C., & Tworek, H. (2021). Stopping the hostile online attacks hurled at candidates. *Policy Options.*
6. Wagner, A. (2020). Tolerating the trolls? gendered perceptions of online harassment of politicians in Canada. *Feminist Media Studies*, 1–16.
7. Amnesty International (2020). Troll patrol findings. *Troll Patrol Report.*
8. Harmer, E., & Southern, R. (2021). Digital microaggressions and everyday othering: An analysis of tweets sent to women members of Parliament in the UK. *Information, Communication & Society*, 24(14), 1998–2015.
9. Technical Division, UNFPA. (2021). Making all spaces safe. *UNFPA.*
10. United Nations General Assembly. (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. Dubravka Šimonović.
11. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence.
12. Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S., & Kaufman, Z. (2021). Maligned Creativity - Wilson Center. *Wilson Center.*
13. Ibid.
14. Ibid.
15. Ibid.
16. Ibid.
17. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
18. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence.
19. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA.*
20. Denny, J. (2020). What is an algorithm? how computers know what to do with data. *The Conversation.*
21. IBM Cloud Education (2020). Artificial Intelligence (AI). IBM.
22. Himelein-Wachowiak, M., Giorgi, S., Devoto, A., Rahman, M., Ungar, L., Schwartz, H.A., Epstein, D. H., Leggio, L., & Curtis, B. (2021). Bots and Misinformation Spread on Social Media: Implications for COVID-19. *Journal of medical Internet research*, 23(5).

23. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence.
24. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
25. Ibid.
26. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
27. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
28. Technical Division, UNFPA. (2021). Making all spaces safe. *UNFPA*.
29. Ibid.
30. Ibid.
31. Ibid.
32. Ibid.
33. Levitsky, S. & Ziblatt, D. (2019). *How Democracies Die*. Broadway Books.
34. Ibid.
35. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
36. Levitsky, S. & Ziblatt, D. (2019). *How Democracies Die*. Broadway Books.
37. Ibid.
38. Bridoux, J., & Kurki, M. (2014). *Democracy promotion: a critical introduction*. Routledge.
39. Clinton, H. R. (1999). Remarks and commentary by first lady Hillary Rodham Clinton--vital voices, 1997-1999. Executive Office of the President.
40. McGreal, C. (2012.) Arab Women Fights to Keep Gains Won on the Street. *The Guardian*.
41. Chenoweth, E., & Zoe Marks. (2022). Revenge of the Patriarchs: Why Autocrats Fear Women. *Foreign Affairs*.
42. Ibid.
43. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence.
44. Ibid.
45. Ibid.
46. Ibid.
47. United Nations General Assembly. (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. Dubravka Šimonović.
48. Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755.
49. Chenoweth, E., & Zoe Marks. (2022). Revenge of the Patriarchs: Why Autocrats Fear Women. *Foreign Affairs*.

50. Ibid.
51. Donegan, R. (2012). Bullying and cyberbullying: History, statistics, law, prevention and analysis. *The Elon Journal of Undergraduate Research in Communications*, 3(1), 34.
52. Ibid.
53. Ibid.
54. Ibid.
55. Donegan, R. (2012). Bullying and cyberbullying: History, statistics, law, prevention and analysis. *The Elon Journal of Undergraduate Research in Communications*, 3(1), 35.
56. Ibid.
57. Ibid.
58. Winkelman, Sloane, Jody Oomen-Early, Ashley D. Walker, Lawrence Chu, Alice Yick-Flanagan. 2015. "Exploring Cyber Harassment among Women Who Use Social Media." *Universal Journal of Public Health*, 3 (5): 194-201.
59. Ejaz, B., & Imtiaz, S. (2015). Sexual harassment: A study of mal-adaptation of information and communication technology. *The Explorer: Journal of Social Sciences*, 1(3), 58-61.
60. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
61. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 18.
62. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 16.
63. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 25.
64. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
65. Ibid.
66. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 24.
67. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 25.
68. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 26.
69. Ibid.
70. Ibid.
71. Jane, E. A. (2016). Misogyny online : A short (and brutish) history. *SAGE Publications*, p. 29.
72. Ibid.
73. Ibid.
74. Kishi, R. (2021). Violence Targeting Women in Politics: Trends in Targets, Types, and Perpetrators of Political Violence. *ACLED*.
75. Ibid.
76. Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755.

77. Kishi, R. (2021). Violence Targeting Women in Politics: Trends in Targets, Types, and Perpetrators of Political Violence. *ACLEDA*.
78. Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755.
79. Ibid.
80. Ibid.
81. Blume, L. R. (2017). The old rules no longer apply: Explaining narco-assassinations of Mexican politicians. *Journal of Politics in Latin America*, 9(1), 59–90.
82. International Foundation for Electoral Systems. (2021). Assessment of Online Violence Against Politically and Civically Engaged Women in Bangladesh. *International Foundation for Electoral Systems*.
83. Ibid.
84. Ibid.
85. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
86. Ibid.
87. Reich, R. (2021). What Happens When a Congressman Threatens a Colleague With Violence. *The Guardian*.
88. Ibid.
89. Ibid.
90. Kishi, R. (2021). Violence Targeting Women in Politics: Trends in Targets, Types, and Perpetrators of Political Violence. *ACLEDA*.
91. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
92. Yasir, S. (2022). Online ‘Auction’ Is Latest Attack on Muslim Women in India. *The New York Times*.
93. Ibid.
94. Ibid.
95. Ibid.
96. Ibid.
97. Ibid.
98. Specia, M. (2019). Threats and Abuse Prompt Female Lawmakers to Leave U.K. Parliament. *The New York Times*.
99. Ibid.
100. Ibid.
101. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.

102. Harmer, E., & Southern, R. (2021). Digital microaggressions and everyday othering: An analysis of tweets sent to women members of Parliament in the UK. *Information, Communication & Society*, 24(14), 1998–2015.
103. Ibid.
104. Erikson, J., Håkansson, S., & Josefsson, C. (2021). Three Dimensions of Gendered Online Abuse: Analyzing Swedish MPs' Experiences of Social Media. *Perspectives on Politics*, 1–17.
105. Ibid.
106. Ibid.
107. Ibid.
108. Ibid.
109. The Economist Intelligence Unit. (2021). Measuring the prevalence of online violence against women.
110. Abdul-Hassan, Ali and Salaheddin, Sinan. (2018). Despite Challenges, Iraq's Female Candidates Run for Parliament. *Christian Science Monitor*.
111. Ibid.
112. Keating, J. (2009). Orthodox Paper Photoshops Women Out of Israeli Cabinet. *Foreign Policy*.
113. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
114. Ibid.
115. Hassan, F. M., Khalifa, F. N., El Desouky, E. D., Salem, M. R., & Ali, M. M. (2020). Cyber violence pattern and related factors: online survey of females in Egypt. *Egyptian journal of forensic sciences*, 10(1), 1-7.
116. Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755.
117. Kakande, A., Achieng, G., Iyer, N., Nyamwire, B., Nabulega, S., & Mwendwa, I. (2021). Amplified Abuse: Report on Online Violence Against Women in the 2021 Uganda General Election. *Pollicy*.
118. Ibid.
119. Ibid.
120. Ibid.
121. Ibid.
122. Ibid.
123. Ibid.
124. Ibid.
125. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
126. Iyer, B. Nyamwire & S. Nabulega (2020) Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet, Pollicy.

127. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
128. Every-Palmer, S., Barry-Walsh, J., & Pathé, M. (2015). Harassment, stalking, threats and attacks targeting New Zealand politicians: A mental health issue. *Australian & New Zealand Journal of Psychiatry*, 49(7), 634–641.
129. Ibid.
130. Ibid.
131. Davies, L. (2014). Laura Boldrini: The Italian Politician Rising above the Rape Threats. *The Guardian*.
132. Ibid.
133. International Foundation for Electoral Systems. (2021). Assessment of Online Violence Against Politically and Civically Engaged Women in Bangladesh. *International Foundation for Electoral Systems*.
134. Ibid.
135. Ibid.
136. Lamensch, M. (2021). When Women Are Silenced Online, Democracy Suffers. *Centre for International Governance Innovation*.
137. Ibid.
138. Project Someone. (2019). Online Misogyny in Canadian Politics.
139. Ibid.
140. Ibid.
141. Ibid.
142. Astor, M. (2018). For Female Candidates, Harassment and Threats Come Every Day. *The New York Times*.
143. Ibid.
144. Ibid.
145. Brechenmacher, S., & Di Meco, S. (2020). Tackling Online Abuse and Disinformation Targeting Women in Politics. *Carnegie Endowment for International Peace*.
146. Hunt, E., Evershed, N., & Liu, R. (2016). From Julia Gillard to Hillary Clinton: Online abuse of politicians around the world. *The Guardian*.
147. Ibid.
148. Astor, M. (2018). For Female Candidates, Harassment and Threats Come Every Day. *The New York Times*.
149. Ibid.
150. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
151. Ibid.
152. Ibid.

153. Ibid.
154. Inter-Parliamentary Union. (2018). Sexism, harassment and violence against women parliamentarians. *Council of Europe*.
155. Ibid.
156. Ibid.
157. Ibid.
158. Harmer, E., & Southern, R. (2021). Digital microaggressions and everyday othering: An analysis of tweets sent to women members of Parliament in the UK. *Information, Communication & Society*, 24(14), 1998–2015.
159. Specia, M. (2019). Threats and Abuse Prompt Female Lawmakers to Leave U.K. Parliament. *The New York Times*.
160. Iyer, B. Nyamwire & S. Nabulega (2020) Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet, Pollicy.
161. Francisco, S. C., & Felmlee, D. H. (2022). What Did You Call Me? An Analysis of Online Harassment Towards Black and Latinx Women. *Race and Social Problems*, 14(1), 1–13.
162. Ibid.
163. Lamensch, M. (2021). When Women Are Silenced Online, Democracy Suffers. *Centre for International Governance Innovation*.
164. Brechenmacher, S., & Di Meco, S. (2020). Tackling Online Abuse and Disinformation Targeting Women in Politics. *Carnegie Endowment for International Peace*.
165. Robinson, A., Piay-Fernandex, N., Baird, S., Jubbero, M., Minott, D., & Larnerd, J. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe. *Technical Division, UNFPA*.
166. Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S., & Kaufman, Z. (2021). Malign Creativity - Wilson Center. *Wilson Center*.
167. Brechenmacher, S., & Di Meco, S. (2020). Tackling Online Abuse and Disinformation Targeting Women in Politics. *Carnegie Endowment for International Peace*.
168. Tumulty, K., Woodsome, K., & Peçanha, S. (2020). Opinion | how sexist, racist attacks on Kamala Harris have spread online - a case study. *The Washington Post*.
169. Heilweil, R. (2020). Why Algorithms Can Be Racist and Sexist. *Vox*.
170. Resnick, B. (2019). Yes, Artificial Intelligence Can Be Racist. *Vox*.
171. Sobieraj, S. (2020). Credible Threat: Attacks against Women Online and the Future of Democracy. *Oxford University Press*.
172. Atalanta (2018). (Anti) Social Media: The Benefits and Pitfalls of Digital for Female Politicians.
173. Rabson, M. (2019). Threats, abuse move from online to Real World, McKenna now requires security. *CTVNews*.
174. Astor, M. (2018). For Female Candidates, Harassment and Threats Come Every Day. *The New York Times*.

175. Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755.
176. Tenove, C., & Tworek, H. (2021). Stopping the hostile online attacks hurled at candidates. *Policy Options*.
177. Kakande, A., Achieng, G., Iyer, N., Nyamwire, B., Nabulega, S., & Mwendwa, I. (2021). Amplified Abuse: Report on Online Violence Against Women in the 2021 Uganda General Election. *Pollicy*.
178. Sobieraj, S. (2020). Credible Threat: Attacks against Women Online and the Future of Democracy. *Oxford University Press*.
179. Wagner, A. (2020). Tolerating the trolls? gendered perceptions of online harassment of politicians in Canada. *Feminist Media Studies*, 1–16.
180. Ibid.
181. Matfess, H., Kishi, R., & Berry, M. E. (2022). No safety in numbers: Political representation and political violence targeting women in Kenya. *International Feminist Journal of Politics*, 1–23.
182. Lamensch, M. (2021). When Women Are Silenced Online, Democracy Suffers. *Centre for International Governance Innovation*.
183. Ibid.
184. Amnesty International (2020). Troll patrol findings. *Troll Patrol Report*.
185. National Democratic Institute. (2021). #NotTheCost - Stopping Violence Against Women in Politics: A Renewed Call to Action. Washington, DC.
186. Lilleker, D., Koc-Michalska, K., & Bimber, B. (2021). Women learn while men talk?: Revisiting gender differences in political engagement in online environments. *Information, Communication & Society*, 24(14), 2037–2053.
187. Nadim, M., & Fladmoe, A. (2019). Silencing women? gender and online harassment. *Social Science Computer Review*, 39(2), 245–258.
188. Lilleker, D., Koc-Michalska, K., & Bimber, B. (2021). Women learn while men talk?: Revisiting gender differences in political engagement in online environments. *Information, Communication & Society*, 24(14), 2037–2053.
189. Sobieraj, S. (2017). Bitch, Slut, skank, Cunt: Patterned resistance to women’s visibility in Digital Publics. *Information, Communication & Society*, 21(11), 1700–1714.
190. Barker, K., & Jurasz, O. (2021). Text-based (sexual) abuse and online violence against women: Toward law reform? *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 247–264.
191. Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S., & Kaufman, Z. (2021). Malign Creativity - Wilson Center. *Wilson Center*.
192. Ferrier, M., & Garud-Patkar, N. (2018). Trollbusters: Fighting online harassment of women journalists. *Mediating Misogyny*, 311–332.
193. The United States Government. (2021). Summit for democracy summary of proceedings. Washington, DC: The White House.

194. Brechenmacher, S., & Mann, K. (2022). Renewing U.S. investments in women's political leadership. *Just Security*.
195. Mendoza, C., & Zurka, K. (2022). The summit for democracy: Advancing gender equity and equality for Representative Societies - United States Department of State. Washington, DC: U.S. Department of State.
196. Biden Campaign. (2020). Joe Biden's plan to end violence against women. *Joe Biden for President: Official Campaign Website*.
197. The United States Government. (2022). Fact sheet: Biden-Harris Administration celebrates first anniversary of the establishment of the White House Gender Policy Council. *The White House*.
198. Biden Campaign. (2020). Joe Biden's plan to end violence against women. *Joe Biden for President: Official Campaign Website*.
199. Squires, C. (2022). US cities are increasing funding for police, with Biden's blessing. *Quartz*.
200. Office of the Spokesperson. (2022). 2022 roadmap for the global partnership for action on gender-based online harassment and abuse. *U.S. Department of State*.
201. Australian Government. (n.d.). About the commissioner | Esafety commissioner. *eSafety Commissioner*.
202. Australian Government. (n.d.). Our legislative functions. *eSafety Commissioner*.
203. Australian Government. (n.d.). Our legislative functions. *eSafety Commissioner*.
204. Kwan, C. (2022). E-safety outlines long list of challenges within Australia's proposed anti-trolling laws. *ZDNet*.
205. Ministry of Foreign Affairs of Denmark. (2021). The Tech for Democracy initiative. *UM*.
206. Ibid.
207. Clontz, C. (2020). Violence against women in politics in Bolivia. *Panoramas*.
208. Krook, M. L., & Restrepo Sanín, J. (2020). The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians. *Perspectives on Politics*, 18(3), 740–755.
209. Ibid.
210. General Data Protection Regulation (GDPR). (2018). *General Data Protection Regulation (GDPR)*.
211. Ibid.
212. Carry, G. (2019) At the GDPR's First Anniversary, the Impact on US Companies Grows. *Data Law Insights*,
213. Mchangama, J., & Fiss, J. (2019). Germany's online crackdowns inspire the world's dictators. *Foreign Policy*.
214. Ibid.
215. Ibid.
216. Technical Division, UNFPA. (2021). Making all spaces safe. *UNFPA*.
217. Norton, J. (2022). Online safety bill will force web giants to protect users from fraud and hate crimes. *Daily Mail Online*.

218. Terry, K. (2022). Tory MP Maria Miller tells how she was cyber-flashed while on busy train into Waterloo. *Daily Mail Online*.
219. Lindström, N. (2019). Think you're being abused by a sexist troll? It could be a bot. *New Matilda*.
220. Ibid.
221. Big Brother Watch. (2021). The State of Free Speech Online. *Big Brother Watch: Defending Civil Liberties, Protecting Privacy*.
222. Technical Division, UNFPA. (2021). Making all spaces safe. *UNFPA*.
223. Kwan, C. (2022). E-safety outlines long list of challenges within Australia's proposed anti-trolling laws. *ZDNet*.
224. Areto Labs. (n.d.).
225. Ibid.
226. Axline, A. (2022). Areto Labs: Using technology to combat online toxicity. *About Alberta Tech*.
227. Ramalingam, V., & Frenett, R. (2022). Our Approach. *Moonshot*.
228. Stinson, M., & Gladstone, N. (2019). Community voices: Mobilizing for women's rights in North Africa. *RightsCon Summit Series*.
229. Al Jazeera. (2018). Morocco criminalises violence against women and sexual harassment. *Women's Rights News | Al Jazeera*.
230. Human Rights Watch. (2022). Turkey defies international human rights law. *Human Rights Watch*.
231. Karakas, B. (2020). Turkey: Laws against domestic abuse fail to protect women. *DW.COM*.
232. Manjoo, F. (2018). The problem with fixing WhatsApp? Human nature might get in the way. *The New York Times*.
233. Onyango, E. (2021). Kenyan influencers paid to take 'guerrilla warfare' online. *BBC News*.
234. Manjoo, F. (2018). The problem with fixing WhatsApp? Human nature might get in the way. *The New York Times*.
235. Lindström, N. (2019). Think you're being abused by a sexist troll? It could be a bot. *New Matilda*.
236. Himelein-Wachowiak, M., Giorgi, S., Devoto, A., Rahman, M., Ungar, L., Schwartz, H.A., Epstein, D. H., Leggio, L., & Curtis, B. (2021). Bots and Misinformation Spread on Social Media: Implications for COVID-19. *Journal of medical Internet research*, 23(5).
237. Lindström, N. (2019). Think you're being abused by a sexist troll? It could be a bot. *New Matilda*.
238. Wijnhoven, F., & van Haren, J. (2021). Search engine gender bias. *Frontiers*.
239. McQuate, S. (2022). Google's 'CEO' image search gender bias hasn't really been fixed. *UW News*.
240. Horwitz, J. (2021). Facebook algorithm shows gender bias in job ads, study finds. *The Wall Street Journal*.
241. The Office for Victims of Crime Training and Technical Assistance Center. (2022). Human trafficking task force e-guide. *OVC TTAC: Office for Victims of Crime Training & Technical Assistance Center*.
242. U.S. Department of State. (2021). Unifying Trauma-Informed Practices and Voices of Survivor Leadership. *U.S. Department of State*.

243. The Office for Victims of Crime Training and Technical Assistance Center. (2022). Human trafficking task force e-guide. *OVC TTAC: Office for Victims of Crime Training & Technical Assistance Center*.
244. State Department. (2018). Implementing a trauma-informed approach.
245. Renaissance. (2019). What is Digital Literacy and why does it matter? *Renaissance Blog*.
246. Interagency Security Committee. (2013). The risk management process for federal facilities. *CISA*.
247. The United States Government. (2022). Fact sheet: President's Interagency Task Force to Monitor and combat trafficking in persons. *The White House*.
248. Vagianos, Alanna. (2019). The Rape Kit Backlog Shows Exactly How We Regard Women In This Country. *Huffpost*.
249. GIFCT. (2022). What we do: Tech innovation. *GIFCT*.
250. GIFCT. (2022). Who we are: About. *GIFCT*.
251. OAS. (2018). Anti-money laundering. *CICAD*.
252. Ibid.
253. Office of the United States Trade Representative (USTR). (2022). 2022 Trade Policy Agenda &
254. Bureau of International Labor Affairs. (2022). Labor Rights and the United States-Mexico-Canada Agreement (USMCA).
255. The United States Government. (2022). Fact sheet: Biden-Harris Administration celebrates first anniversary of the establishment of the White House Gender Policy Council. *The White House*.
256. Office of Press Relations. (2021). USAID announces initiatives to advance democracy in support of Presidential Initiative for Democratic Renewal: Press Release. *U.S. Agency for International Development*.
257. House of Representatives, H. R. 2154 (2021). Congress.
258. Senate and House of Representatives, S.1896, H.R.3611 (2021).
259. Tcheng, H. (2020). Tech due diligence: The new pillar of M&A activity. *BearingPoint USA*.
260. United States Government. (2021). The National Action Plan to Combat Human Trafficking. *White House*.