Impacts, Lessons Learned, and Best Practices for Supporting Knowledge Workers Targeted by Online Abuse:

A Knowledge Synthesis Report

Impacts, leçons apprises, et meilleures pratiques pour assister au soutien des travailleurs du savoir ciblés par la maltraitance en ligne:

Un Rapport De Synthèse

August 2021

Impacts, Lessons Learned, and Best Practices for Supporting Knowledge Workers Targeted by Online Abuse:

A Knowledge Synthesis Report is co-funded by the Social Sciences and Humanities Research Council and the Government of Canada's Future Skills program

Impacts, leçons apprises, et meilleures pratiques pour assister au soutien des travailleurs du savoir ciblés par la maltraitance en ligne:

Un rapport de synthèse des connaissances est cofinancé par le Conseil de recherches en sciences humaines et le programme Compétences futures du Gouvernement du Canada.

Social Sciences and Humanities Research Council of Canada

Conseil de recherches en sciences humaines du Canada

BY

Chandell Gosse (she/her)
Postdoctoral Research Associate, College of Interdisciplinary Studies, Royal Roads University

Victoria O'Meara (she/her)
PhD candidate, Media Studies, Western University

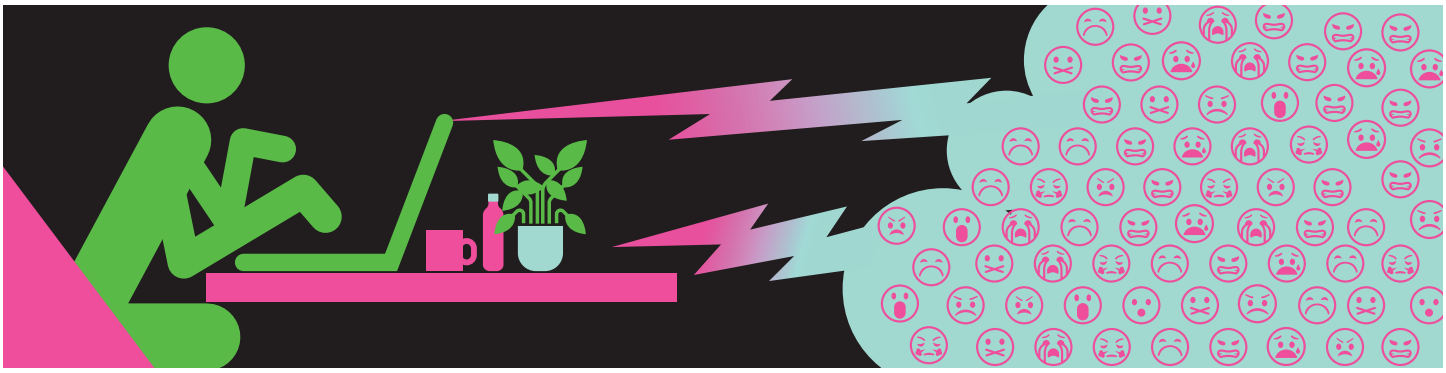
Andrea Galizia (she/her)
JD candidate, Osgoode Hall Law School, York University

Jaigris Hodson (she/her)
Associate Professor, College of Interdisciplinary Studies, Royal Roads University
Canada Research Chair, Digital Communication for the Public Interest

TABLE OF CONTENTS

TABLE OF CONTENTS cont.

EXECUTIVE SUMMARY



BACKGROUND

Digital communication technologies (DCTs) have become critical venues for the public to access, share, and discuss information, news, and entertainment. This is true now more than ever, as the COVID-19 pandemic has expanded and accelerated the integration of digital platforms into our daily lives. Many have come to rely upon these tools for work, school, socializing, and meeting basic needs.

For researchers and research communicators, digital tools have become essential to how they conduct research, share their work, engage with the public, and collaborate with others in their field. However, online abuse has emerged as a serious obstacle that undermines the potential of digital media platforms for research, knowledge mobilization, and innovation.

Research has shown that online abuse can adversely impact targets, encouraging forms of self-censorship and driving people entirely offline (Chadha et al., 2020; Citron, 2014). At a time when knowledge workers are called upon to do most of their work online, this project synthesizes the existing body of work related to the online abuse of knowledge workers in the research and public education fields and provides evidence-based recommendations to guide the organizations that hire them.

OBJECTIVES

This project investigates:

1) the obstacles online abuse presents to those who experience it;
2) the personal and organizational costs of online abuse; and
3) practices that institutions and organizations can incorporate to help workers who experience online abuse.

RESULTS

- Systems of oppression, such as racism, sexism, homophobia, and transphobia, place individuals at a higher risk of online abuse. Other factors, such as one's online visibility and the topic of discussion also put individuals at greater risk of abuse.
- Knowledge workers are primarily dealing with online abuse independently or with the help of their close personal network. Strategies for coping with abuse include fighting back against abuse by responding to perpetrators directly or challenging them publicly and engaging in anticipatory labour to prepare for future attacks.
- Online abuse has significant mental, emotional, and financial impacts on individual targets. The impact of online abuse rever berates outwards to affect communities, organizations, institutions, and the state of public discourse, more broadly.

EXECUTIVE SUMMARY cont.

- Recommendations in the research identify various stakeholders who have a role to play in addressing online abuse, including individual targets; employers; friends, colleagues, and other bystanders; governments and policymakers; platform companies; and the law and law enforcement.

KEY MESSAGES

- The risk factors associated with experiencing online abuse demonstrate the significance of this problem for justice, equity, and innovation. Those most at risk of experiencing online abuse are also most likely to experience oppression and marginalization. Online abuse exacerbates and further entrenches existing social and economic inequities.
- Common responses to experiences of online abuse underscore the fact that this burden is largely shouldered by individuals and their networks. Engaging in forms of "anticipatory labour" to prevent abuse; "quietly coping" by trying to ignore the abuse or filter it out with the help of friends; and "fighting back" by challenging perpetrators directly and publicly are all personal coping strategies that emerge from broader systemic failings. Individuals are bearing the brunt of this problem, in part, because of what we call a pervasive culture of ambiguity surrounding what employers can, will, and should do about online abuse.
- The recommendations made in the research further underscore that, at present, individuals and their networks are being left to fend for themselves and are burdened with the responsibility of managing and responding to the abuse. The recommendations made for individuals also testify to the significant investment of time, energy, and personal resources that individuals are required to make to protect themselves.
- The cost of online abuse is not evenly distributed across social groups. Members of equity-deserving groups are having to invest more heavily in preventing, responding to,and mitigating the damage of online abuse. This constitutes a drain on their resources with serious repercussions for their professional advancement, equity in the workplace, diversity across industries, and innovation across society at large.

METHODOLOGY

We conducted a scoping review, a methodology that involves "contextualiz[ing] knowledge" by evaluating what is known and what is not known about a certain topic, and subsequently applying this knowledge in "policy and practice contexts" (Anderson et al., 2008, p.10). Our scoping review focused on academic and grey literature, including policy papers, news reports, and organizational guidelines relating to online abuse across a wide variety of disciplines.

We searched several online repositories using a list of key terms compiled by the research team and reviewed bibliographies from the literature for further resources. Our initial search returned 245 documents, 43 of which were removed from the dataset based on the project's inclusion/exclusion criteria. Our final sample included 202 documents. Using Nvivo 13, the literature was then coded using an inductive and deductive process.

Full Report

FULL REPORT

INTRODUCTION

Digital communication technologies[1] (DCT) have become critical venues for the public to access, share, and discuss information, news, and entertainment. They have been so thoroughly integrated into everyday life that the use of social media platforms, email, and video conferencing and messaging apps have become a tacit expectation for workers in a variety of industries across the knowledge economy.[2] For instance, journalists, academics, public health and government officials, science communicators, and workers in the non-profit sector are increasingly expected to utilize social media to conduct research and share their work (Amnesty International, 2018; Melovic et al., 2020; Gosse et al., 2021). For these knowledge workers,[3] DCT are essential for mobilizing their knowledge and engaging with the public.

While the integration of DCTs into our daily lives has been underway for some time, the COVID-19 pandemic has expanded and accelerated this trend. Over the last year, DCTs have become essential tools for work, school, socializing, and meeting basic needs. However, increased use and visibility has its drawbacks: namely, it leaves people vulnerable to online abuse. In this report, we review the extant research to synthesize what is known about online abuse and to recommend practices to better protect and support the workers who experience it.

Online abuse is the misuse of digital communication technologies to harm someone.[4] It can include everything from inappropriate messages and ad hominem attacks to online impersonation and image abuse (Hodson et al., 2018). Online abuse can have damaging consequences for those who experience it; however, targets do not exist in a vacuum.[5] The harms caused by online abuse tend to pervade an individual's greater web of elationships, with consequences for friends, family, and peers. Furthermore, the threat of online abuse impacts how others are willing to engage with DCTs with the potential to curtail diverse participation and innovation.

1 Digital communication technologies include, but are not limited to: email; websites; social media platforms like Twitter and Facebook; video conferencing software like Zoom and Microsoft teams; collaborative work tools like Google Docs and Slack; and messaging services like SMS text, WhatsApp, and Signal.

2 Although notoriously difflcult to deflne (Brinkley, 2006), broadly speaking, the term "knowledge economy" refers to a transition away from an economic model premised largely upon heavy industry and the production of material goods, towards one that centres knowledge, information, and communication (think: from factory work to offlce work).

3 While "knowledge workers" can include anyone whose work requires the application or production of knowledge or information (for example, IT professionals, call center operators), in this report we are concerned this speciflc subset of knowledge workers; those whose work involves conducting research and/or communicating research and information to the public.

4 Digital communication technologies include, but are not limited to, social media platforms, including game platforms, email, smartphones, the Internet of things [IoT], and digital images and video.

5 We use the term 'target' to refer to someone who experiences online abuse. We prefer this term to applying the label of 'victim' without flrst understanding whether the affected individual identifles as a victim.

CONTEXT

Online abuse can involve inappropriate comments and harassing messages (Jane, 2014), image abuse, such as the non-consensual distribution of intimate images (McGlynn and Rackley, 2017a) or up-skirting (McGlynn and Rackley, 2017b), privacy-related offences, such as the disclosure of personal or private information, known as doxing (Eckert and Metzger-Riftkin, 2020), and disruption to people's online profiles or websites through hacking (Massanari, 2015), and DDoS attacks (Traer and Bednar, 2021). These are only a few examples. Online abuse consists of a spectrum from mild to very severe and not all instances of abuse cause harm in the same way. One of the difficulties of defining online abuse comes from how quickly new forms of abuse emerge. For instance, in the last two years concerns over deepfakes and abuse via the internet of things (IoT) have emerged (Slupska and Tanczer, 2021).[6] In the last year alone, we have witnessed the development of 'zoombombing' (Elmer, Burton, and Neville, 2020), a type of abuse that stems from our move to working from home and connecting remotely via online video conferencing tools.

While as recently as 2014, Jane noted that there is a lack of research on the topic of online abuse, this has since changed dramatically. There is now a substantial body of research that underscores the prevalence of online abuse across varying online contexts. For example, two recent large-scale US-based surveys reported that over 40% of respondents experienced some form of online abuse (Lenhart et al., 2016). A similar study found that 31% of Canadian social media users had experienced online abuse (Angus Reid, 2016). Likewise, in a study of 121 faculty at a Canadian university, Cassidy, Faucher, and Jackson (2014) found that over 17% of respondents had experienced some form of online abuse.

This evidence suggests that online abuse has become a common consequence of internet use. In addition, experiences of online abuse are on the rise. In 2014, Pew Research Center found that 35% of American adults had experienced online abuse (Duggan, 2014). This number grew to 41% in a 2017 study (Duggan, 2017b). In their most recent work, researchers at Pew found evidence to suggest that the abuse has become more extreme (Desilver, 2021). Pew Research Center's 2021 study found that although the number of people that report experiencing online abuse has remained fairly stable since 2017, the number of individuals that experience severe forms of abuse, as well as multiple forms of harassing behaviors, has dramatically increased.

Social media is a venue where online abuse commonly occurs. For instance, one study found that the percentage of respondents that said their most recent harassing encounter occurred on social media grew substantially from 58% in 2017 to 75% in 2020 (Vogels, 2021). But online abuse often also occurs through other communication technologies, such as email. Previous research found that 42% of surveyed academics experienced abuse via email (Gosse et al., 2021) — a troubling statistic considering that email has become essential for workers across industries.

6 A deepfake combines the face of one person and the body of another to generate a third, composite video that shows a person doing or saying something they have not actually done or said (For examples of how deepakes are harmful, see Gosse and Burkell, 2020). The Internet of Things (IoT) describes how everyday objects are increasingly equipped with an internet connection that allows them to send data between objects. Examples include smart home devices like Amazon Echo, smart thermostats, televisions, and doorbells, to name only a few.

The significant role that DCTs play in the professional and personal lives of knowledge workers cannot be overstated. As digital technologies become more deeply embedded into the way that we work and live, staying offline to avoid abuse becomes an increasingly untenable solution. A growing portion of the population cannot afford to stop using DCTs (Gosse, 2021).

Given this relationship, there is a strong imperative to direct our attention to understanding how better to support and protect people from online abuse. This report contributes to this imperative by reviewing extant research to better understand what we know about online abuse to date and recommending practices to better support workers.

OBJECTIVES

The experience of online abuse places undue economic, social, and emotional burdens on targets. These burdens are exacerbated when the target relies on virtual platforms for work. Mounting an appropriate response to this problem begins with investing adequate attention into understanding the existing research on online abuse. Such work is necessary to provide adaptive solutions.

The goal of this synthesis report is to help Canadian institutions and organizations adapt to the digital knowledge economy. At a time when research and public education workers are called to do most of their work through social media and related technologies, this project synthesizes the existing body of work related to the online abuse of knowledge workers in the research and public education fields and provides evidence-based recommendations to guide the organizations that hire them.

Specifically, this project investigates

1) The obstacles online abuse presents to those who experience it;
2) The personal and organizational costs of online abuse; and,
3) Practices that institutions and organizations can incorporate to help workers who experience online abuse.[7]

To guide these objectives, we asked the following four research questions:

1) What does the current academic and grey literature recommend for protecting knowledge workers doing research and public education work from online abuse?
2) What are the consequences for worker engagement when knowledge workers experience online abuse; how does the experience of abuse impact society in a (now) digital workplace?
3) What consequence does online abuse have for diversity and inclusion in the knowledge economy?
4) What immediate steps do Canadian knowledge workers, their employers, and policymakers need to take to protect workers and support innovation, knowledge mobilization, and collaboration in an increasingly digital knowledge economy?

7 We use the term 'institution' to refer to larger establishments such as social media platforms and law and law enforcement. We use the term 'organization' to refer to employers and places of work.

METHODOLOGY

To answer the research questions, we conducted a scoping review. Scoping review methodology seeks to "contextualiz[e] knowledge" by evaluating what is known and what is not known about a certain topic, and subsequently applying this knowledge in "policy and practice contexts" (Anderson et al., 2008, p.10). This method served two primary purposes: first, to provide a synthesis of existing work on online abuse that relates to knowledge workers in the research and public education fields; and second, to provide evidence-based recommendations to guide organizations that hire these workers. To meet these goals, the scoping review focused on academic and grey literature, including policy papers, news reports, and organizational guidelines relating to online abuse across a wide variety of disciplines. Our approach was informed by the original scoping review framework, developed by Arksey and O'Malley (2005) and later clarified by Levac et al. (2010) and researchers at the Joanna Briggs Institute (Peters et al., 2015). The framework includes the following five stages: identifying the research question; identifying relevant studies; study selection; charting the data; and, collating, summarizing, and reporting the results.

IDENTIFYING THE RESEARCH QUESTIONS

Our research questions followed our team's previous work (Gosse, 2021; Gosse et al., 2021; Hodson, Gosse, and Veletsianos, 2021; Hodson et al., 2018; Houlden et al., 2021; Veletsianos et al., 2018). We developed research questions based on our continued findings that online abuse, particularly for those people engaged in academic work, can be best understood using an ecological framework that integrates individual, organizational, sectoral, political, and cultural actions that either exacerbate or help to address issues of abuse. For this reason, our research questions focus on what support and protections exist and how they can be better implemented by institutions, organizations, and workers.

METHODS: IDENTIFYING RELEVANT STUDIES

To frame our search and data collection, we first compiled a list of key terms that describe the DCTs where abuse occurs (Table 1 column A), the harm targets' experience (Table 1 column B), and the populations/targets of interest (Table 1 column C). At this stage, we cast a wide net and included anything that seemed relevant. Only later did we screen documents using our inclusion/exclusion criteria outlined below (see Study Selection section).

Next, we searched several online repositories using a combination of terms from columns A, B, and C. The initial search focused on combinations of A and B. We then conducted a narrower search using a combination of A, B, and C. The online repositories included library databases at Royal Roads University, Western University, and the University of Toronto, as well as Google Scholar, LexisNexis, Factiva, government websites, and search engines (Google, Bing, and DuckDuckGo). Last, we reviewed the bibliographies of the collected research for further resources. In total, our initial search process returned 245 documents.

TABLE 1: KEY TERMS USED IN DATA COLLECTION

A: LOCATION	B: HARM	C: TARGET
Cyber	Violence	Academics / Scholars
Online	Harrassment	Civil Society / Organizations
Social / Social Media (Facebook, Twitter, Instagram)	Bullying	Government / Public Servants
Electronic	Doxing / Doxxing	Politicians
Networked	Stalking	Lawyers / Judges
Technology / Tech	Intimidation	LGBTQIA+
Digital	Trolling	Researchers
	Abuse	Scientists / Doctors
		Video Game Workers
		Women

STUDY SELECTION

After the initial search, we reviewed each document on its own to ensure it met our inclusion criteria. To be included, online abuse had to be the primary focus of the document—if online abuse was only tangentially mentioned it was removed. We also used our research questions to guide inclusion, ensuring that each article touched on support and protection (or lack thereof) or impact and consequences. In the end, 43 documents were removed from our dataset for a total sample of 202.

This dataset is openly available in fig share at:

- https://www.doi.org/10.6084/m9.figshare.15167115

CHARTING THE DATA AND DATA ANALYSIS

Data analysis included a deductive and inductive approach. The first phase of analysis involved charting the data (Levac et al., 2010), whereby members of the research team coded all 202 documents according to eight categories that were generated based on the research questions (see Table 2).

For phase two, we imported the documents from each category into Nvivo 13. The first round of coding in Nvivo 13 involved reviewing a subset of the research (25% for a total of 51 documents) to generate a list of key themes (or categories). Using an inductive and iterative process of constant comparison, members of the team achieved intercoder reliability by discussing, negotiating, and refining the final list of subcodes. The second round of coding in Nvivo 13 involved applying the finalized list of subcodes for each of the phase one categories to the remainder of the dataset.

TABLE 2: PHASE ONE DATA ANALYSIS CODES AND DESCRIPTIONS

CODE	DESCRIPTION
Impact / Consequences	What are the consequences for people concerning work, school, social life, and public participation? What is the impact on broader society? What is the impact on research innovation?
Response	How do institutions, organizations, and people respond to experiencing online abuse?
Recommendations	What recommendations are made to prevent online abuse or support targets?
Efficacy	How successful have responses been?
Risk Factors	What factors put people at risk of experiencing online abuse?
Knowledge gaps	What knowledge gaps does the document identify?
Significance of DCTs	What function/importance does the document assign to DCTs?
Types of abuse	Specific examples of the kinds of abuse people experience.

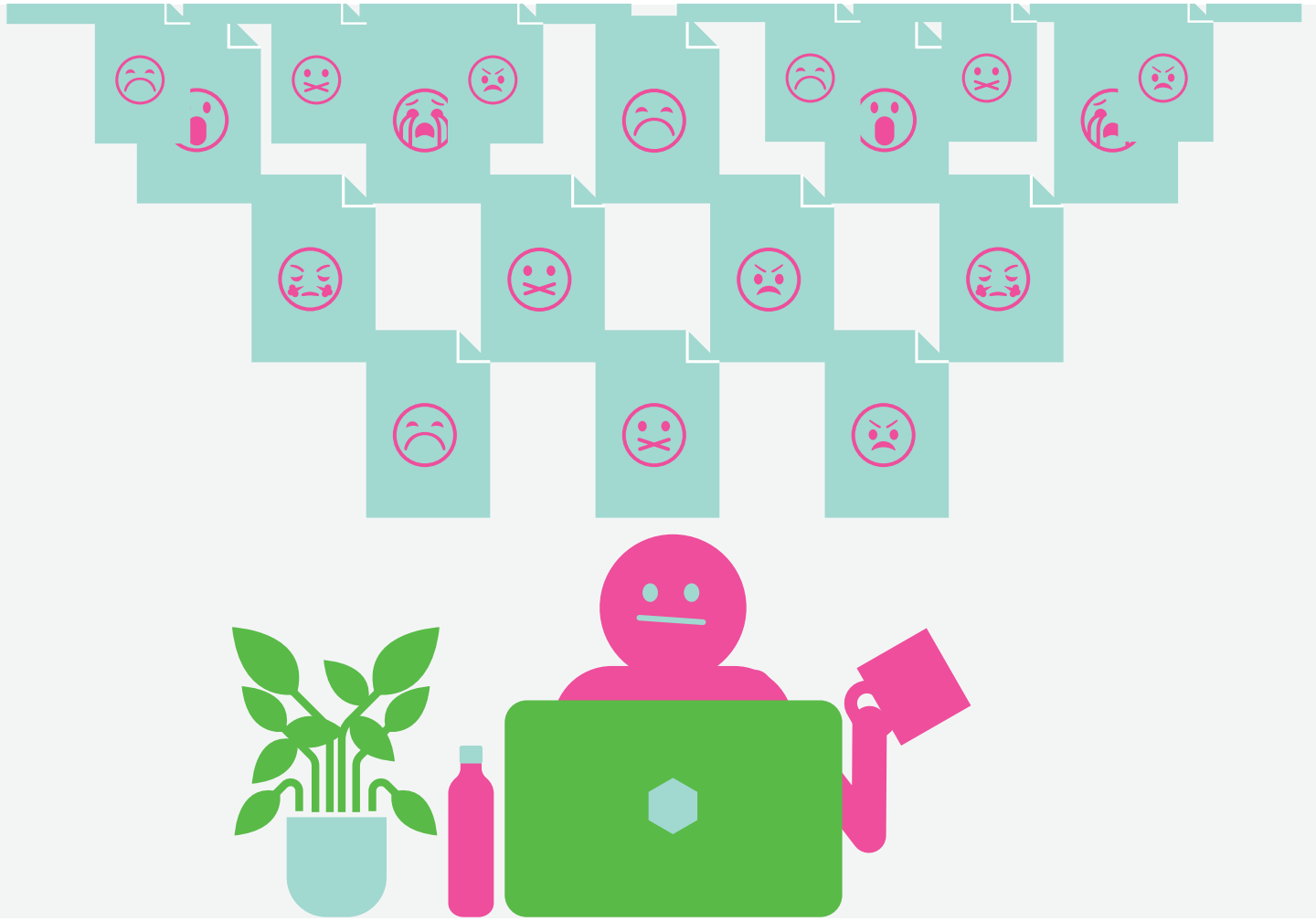
FULL REPORT

COLLATING, SUMMARIZING, AND REPORTING THE RESULTS

Once data analysis was completed, members of the research team wrote summary findings for each subcode. From there the team discussed the significance of the findings and began to outline the contours of this report.

LIMITATIONS OF THE DATA

We identified two limitations to our data: First, because the data used in a scoping review varies in research methodology, we do not adjudicate the quality of the data collected or address the significance of the data presented (Arksey and O'Malley, 2005). Instead, we only provide a descriptive account of the data. Secondly, our findings can only reflect what research is available to us. However, what is available to us may not paint the full picture, and limitations in the original articles can become limitations in our work.



RESULTS

A review of the academic and grey literature shows that online abuse has ramifications far beyond the targeted individual. Online abuse affects communities, organizations, and the health of a functioning democratic society. In this section we report on five areas of research findings that help illuminate the consequences of online abuse for workers of the knowledge economy:

1) the risk factors associated with experiencing online abuse;
2) the impact and consequences of online abuse;
3) responses to abuse;
4) recommendations to support and protect workers; and,
5) knowledge gaps within the research. Each area is broken down into subsections that provide more nuance and meaning to the research. Each subsection has codes or themes of its own, for which we provide the frequency that it was coded in the research.

RISK FACTORS

Workers in the knowledge economy rely on DCTs to conduct their work: social media platforms like Twitter and Facebook, video conferencing software like Zoom and Microsoft teams, and collaborative work tools like Google Docs and Slack have come to serve an important function. Researchers and research communicators use these tools to mobilize their research, educate the public, collaborate and innovate across fields, and generally push society forward. However, the ability to do these things is not equally available to all workers because certain groups are more at risk of experiencing abuse and abuse through DCTs. Our research was thematically grouped to capture three overarching factors that render individuals more vulnerable to online abuse: systems of oppression; the topic spoken or written about; and an individual's circumstance.

SYSTEMS OF OPPRESSION

Racism, sexism, homophobia, transphobia, ableism, xenophobia, and other systems of oppression and discrimination put certain people and groups at a higher risk of being targeted for online abuse.8 Abuse that targets a person's identity was undeniably the most common risk factor in our research. The research consistently indicates that individuals are targeted based on gender identity (n=116), race (n=67), sexuality (n=41), age (n= 14), ability (n=6), socioeconomic status (n=3), or migration background (n=3). Although any one of these alone is sufficient to elevate an individual's risk of online abuse, the research frequently notes that an individual's experience is invariably compounded when they hold an intersectional identity (n=16). For example, patriarchy and racism elevate the likelihood of Black women being targeted for online abuse over that of white women or Black men. The research is consistent in emphasizing the point that individuals who occupy multiple equity-deserving subject positions are at a greater risk than those who occupy only one.

TOPIC

Another factor that puts people at higher risk for online abuse is speaking publicly about certain topics. Topic-driven online abuse is about what a person says: it constitutes abuse that responds to a person sharing their research, writing, opinion, politics, and values. The research indicates that perpetrators target individuals if they take issue with the content of their online posts, as well as for activities they engage in outside of an online context (n=44).[9] This can include political and policy issues such as abortion, gun control, climate change, and Covid-19 vaccines (n=28), or content that catches the attention of far-right and white supremacist groups (n=7). On two occasions, publications noted that calling attention to an incident of online abuse can also exacerbate the abuse (n=2).

RESULTS

CIRCUMSTANCE

The research also included various risk factors that are contextual and associated with a target's particular circumstances. These circumstances shape and inform a person's relationship to DCTs. Unsurprisingly, heightened online visibility, which is broadly defined as having a large online presence, was the most frequently cited risk in this category (n=33). Heightened online visibility is particularly prevalent among public figures (n=7). Other risky circumstances included being precariously employed (n=16) and lacking appropriate training and resources to protect oneself from online harms (n=2). Precarious employment is uniquely related to the risks associated with online abuse. While working as a freelancer or contract worker does not inherently elevate one's risk, this employment situation does generate additional incentives for knowledge workers to participate in online discussion and develop an online presence that marks them as an authority in their field. To secure future employment contracts, this group is under more pressure to engage in aggressive forms of online self-promotion and reputation seeking — more than their colleagues in stable and permanent positions. This puts them at an elevated risk of being targeted for online abuse. This is additionally troubling when considered in combination with the fact that the precariously employed are also constituted disproportionately by women and BIPOC workers (Haque, 2018), who are already at an elevated risk of being targeted for abuse. Furthermore, contract workers are also less likely to have access to the training, protections, and supports that employees have access to, making them additionally vulnerable.[10] Without these supports, individuals are left to fend for themselves, which can exacerbate the impact of online abuse.

IMPACTS AND CONSEQUENCES

The research we examined reveals that online abuse has both damaging impacts on a target's personal and professional life, as well as consequences that reverberate outward to affect broader society.

PERSONAL

Across the research, personal impacts were discussed in six ways. Overwhelmingly, the research underscores that online abuse takes a serious toll on targets' mental and emotional health with negative consequences for an individual's worldview, work, relationships, overall happiness, and quality of life (n=128). Distantly following this, the second most frequently cited personal impact was an elevated concern for one's safety and the safety of their loved ones (n=29), which, at times, burdens targets with the task of seeking out additional protections and enacting additional safety measures (n=3). Third, the research also indicates that online abuse impacts a target's finances, as they shoulder the cost of seeking justice, additional safety, and managing reputational damage (n=19).

8 Physicians and public health experts, including Dr. Camara Phyllis Jones, Dr. Joia Crear-Perry, and Dr. Thomas B. Sequist, have recently challenged the language of the medical establishment that classifles "race" as a risk factor for various health issues (Crear-Perry, 2018; Milano, 2021; Wallis, 2020). As these physicians point out, race is not a risk factor, racism is. In this report we follow their lead, and attempt to use language that draws attention to the systems of oppression that put a person at higher risk, rather than using language that might imply that this risk is inherent to one's race, gender, sexual orientation etc.

9 It is important to note that a person does not need to be online in order to be targeted by online abuse. Offfiine actions, such as media appearances, can lead to online campaigns of abuse and harassment.

RESULTS

PROFESSIONAL

In addition to the detrimental impacts on an individual's personal life, online abuse can damage a person's career and professional life. First, it constrains professional advancement (n=21). For instance, targets of abuse may lose out on opportunities and promotions or be deterred from making career advances or shifts altogether. Second, perpetrators of online abuse sometimes purposely inflict harm on targets by sharing personal information or falsehoods that undermine their credibility and professional reputation (n=20). In these cases, targets are unable to control a narrative that is made publicly accessible to their colleagues, (prospective) employers, and their online community. The reputational harm that an attack can cause is particularly damaging for freelancers and contract workers because it can undermine their future employment opportunities.

As Sobieraj (2020) explains:

> ***[J]ournalists and pundits who do freelance or independent contract work, academics who are untenured or working in adjunct or temporary positions, bloggers and vloggers dependent on advertising revenue, and those in grant- and/or donor-driven nonprofit or activist work are particularly vulnerable to attacks that strive to shame or discredit them*** (p. 95).

Additionally, perpetrators also purposely inflict harm by coordinating online campaigns to have a target fired from their job, oftentimes publicly administering pressure on employers to fire the target (n=14). Finally, dealing with online abuse can cause targets to leave their profession (n=14), and can make it harder for targets to do their job if they do stay because it consumes a significant portion of their time and finite emotional and cognitive resources (n=11).

SOCIETAL

The research demonstrates that the cumulative impact of online abuse has consequences for society and the sphere of public participation. Our scoping review finds that online abuse can disincentivize targets from participating in DCTs (n=96). For example, individuals commonly self-censor in response to online abuse (n=74) and leave or express the desire to leave platforms like social media altogether (n=21). When individuals are deterred from participating in DCTs it constrains the plurality of voices and perspectives, which ultimately harms the public sphere (n=29). This is especially concerning when considered alongside the fact that individuals from equity deserving groups are most likely to experience online abuse.

RESPONSES

Individuals employ a diverse range of responses to the phenomenon of online abuse. Individual responses identified in the research were grouped into three overarching thematic sections: preparing for abuse; quietly coping; and, fighting back. Additionally, the research includes institutional responses from employers.

PREPARING FOR ABUSE

The most common response that individual workers have to online abuse involves behaviors aimed at anticipating, preventing, and mitigating future harms. The most common response to online abuse is for targets to self-censor or reduce their online presence (n=45). Secondly, an individual may respond by pursuing additional safety measures (n=29) such as obtaining a

10 We acknowledge that not all employers offer support and in some cases, employers side with perpetrators or bend to public pressure.

restraining order against an attacker or hiring personal security. Individuals may adjust their work and work environment in preparation for abuse (n=21). For example, Abby Ferber (2018) at the University of Colorado, found that some women educators moved away from teaching controversial subject matter. Lastly, individuals may prepare for abuse by engaging in what Sarah Sobieraj (2020) at Tufts University calls "credibility work" (n=9) (p. 64), such as double and triple-checking sources.

QUIETLY COPING

Individuals deploy a series of coping mechanisms either independently or with the help of their network in response to online abuse. Independent coping mechanisms include deleting abusive comments and blocking abusers (n=16), minimizing the experience of the abuse, or downplaying its harm (n=15), suffering in silence (n=14), or attempting to ignore the abuse (n=11). Coping mechanisms that rely upon personal relationships involve soliciting help from friends, colleagues, and peer networks to respond to attackers, document abuse, or filter out the worst of it (n=37).

FIGHTING BACK

Individuals sometimes challenge online abuse in the following ways: by engaging in advocacy work, such as campaigning to raise awareness about online abuse (n=28); responding directly to attackers and challenging their claims (n=21); or by drawing public attention to the abuse and exposing its perpetrators (n=9).

INSTITUTIONAL RESPONSES

By and large, the research suggests that responses from management or employers of knowledge workers are inadequate or even punitive. These responses include failing to respond to workers reports of online abuse (n=11); prioritizing the organization's public image over that of the target (n=11); distancing the organization from targets of abuse (n=10), dismissing their concerns (n=6), blaming the victim (n=5), terminating the target's employment (n=5), imposing additional constraints on the use of social media (n=2), or telling targets of abuse to simply not respond (n=2).

RECOMMENDATIONS

Recommendations for dealing with online abuse in our scoping review addressed a variety of stakeholders, including individual targets; bystanders such as friends, family, and peers; employers; platform companies; law and law enforcement; as well as governments and policymakers. Each of these has a role to play in combating the problem of online abuse.

The below table (Table 3) provides a breakdown of the number of recommendations made to each of the parties identified above. As we can see, most advice is directed towards the individual who has been targeted for attack. This is followed by employers, bystanders, governments and policymakers, platform companies, and law and law enforcement.

TABLE 3: NUMBER OF RECOMMENDATIONS MADE TO INDIVIDUALS, ORGANIZATIONS, AND INSTITUTIONS

GROUP	n=
Individuals	423
Employers	367
Bystanders, Peers, Colleagues, Friends & Family	116
Governments, Policymakers, and Legal Reforms	91
Platform Companies	83
Law Enforcement, Lawyers & Judges	29

RESULTS

Below we present our findings on recommendations. We begin with a narrow focus on the individual target and move outward to account for the broader sphere of influence that shapes their experience. This includes an individual's network of friends, family, and peers, their employers, and finally, institutions such as law enforcement and platform companies.

BRACE YOURSELF: RECOMMENDATIONS TO INDIVIDUALS

The recommendations for targeted knowledge workers underscore the importance of being prepared for the realities of online abuse. For instance, taking steps to improve one's cybersecurity is the most common recommendation overall (n=111). This is promoted as one important way for individuals to protect themselves against online abuse and mitigate any damage from an attack. Cybersecurity measures are intended to stop future perpetrators from finding and sharing private information or gaining access to and compromising professional websites, social media accounts, online classrooms, and email accounts, to name only a few. These types of recommendations are preparatory and assume that by being proactive individuals can head off the tactics of perpetrators. For instance, knowledge workers are encouraged to use two-factor authentication; upgrade and secure their passwords; review and manage privacy settings on social media; install anti-virus and malware software; install privacy plug-ins to block cookies and other trackers; use a private VPN; disable geo-location; and sign up for data scrubbers to remove personal information from the web. They are also advised to periodically conduct Web searches for their name and images, set up Google Alerts for their name, and monitor comments on their social media.

Beyond tightening their cybersecurity, the second most common recommendation made to individuals is to stop using DCTs (n=57). These recommendations suggest that in the event of an attack individuals log off, shut down their social media, set accounts to private, remove their contact information, think carefully before posting anything personal, and generally, take measures to curtail their visibility online.

The third most common recommendation made to workers is to seek support and prioritize self-care in the event of an experience of online abuse (n=46). Recommendations in this vein encourage targets to avoid isolating themselves; share their experience; seek out members of their social network who can remind them that the abuse is not their fault; speak to a mental health professional; try to get enough sleep; eat well; take breaks from work and DCTs and set aside time for socializing and hobbies.

Existing research frequently advocates that an individual targeted by online abuse should block harassing accounts and report to the platform where the abuse occurred (n=41). Individual targets of abuse are also frequently advised to take steps to document the abuse as evidence for law enforcement so it can be used if the target pursues legal action (n=39). The process of sifting through abusive comments and reporting, blocking, and recording abuse, however, can be a (re)traumatizing experience for targets. As such, individual targets are encouraged to enlist the help of a close friend or colleague to do so (n=36). This ally is meant to act as a digital gatekeeper who reviews incoming messages to filter out abuse and can take over the effort of documenting abuse, blocking abusive accounts and comments, and reporting them to the platform.

RESULTS

In responding to an attack, targets are advised to contact law enforcement if they feel threatened (n=35), to resist the urge to "feed the trolls" (n=24), and to notify their employer of the abuse (n=21). It is also frequently recommended that knowledge workers have a plan in place if abuse does occur, which will help them to mitigate the harm and make the experience feel less overwhelming (n=21). Recommendations in this vein underscore the importance of collaborating with friends or colleagues to prepare a "safety plan" or "emotional action plan" (Online SOS, 2020, p. 2) and familiarizing themselves with the procedures and resources available from their employer.

As one article explained:

> ***While your institution may have some resources, you're going to have to look for them. Ask if your college or university has a media office. Find out if your institution has a protocol in place for threats against its faculty. Look into faculty governance, such as the faculty senate, and ask if they have a clear policy in place about social media and public scholarship. Contact your professional association to see if they have any*** (Stein & Daniels, 2017, p. 156).

Knowledge workers are also advised to always prioritize their physical safety (n=20), and lastly, to seek legal counsel for advice (n=11).

PROVIDING SUPPORT: RECOMMENDATIONS FOR COLLEAGUES, BYSTANDERS, FRIENDS, AND FAMILY

According to the research, the role of friends, colleagues, and bystanders is to provide solidarityand support when they see that someone has become the target of online abuse (n=116). Recommendations for this group involve expressing support through personal messages or public statements; offering to help document or report the abuse; lending a supportive ear; defending the target through counter-speech; advocating on behalf of targets by rallying others; and avoiding victim-blaming or dismissive rhetoric.

BE PROACTIVE AND RESPONSIVE: RECOMMENDATIONS FOR ORGANIZATIONS

At the organizational level, the recommendations from the research can be grouped into three overarching themes that emphasize the importance of:

1) being proactive with policies, procedures, and staff training;
2) supporting targets; and
3) implementing broader organizational changes that are better suited to the realities of digital workplaces.

Current research advocates for clear policies and procedures that respond to online abuse (n=66), as well as equipping workers with the ppropriate education and training to prepare them for the possibility of online abuse (n=65). Indeed, several documents discuss the systemic nature of this problem and urge organizations to wake up to the reality of having to deal with these attacks more frequently in the future (n=16). Any organizational policies should provide social media guidelines for staff, outline the steps workers should take in the event of an attack, and include the forms of protection and support that the organization will provide should a worker be targeted. In the event of an incident, employers are advised to have straightforward abuse reporting mechanisms that are easy for workers to use and can help employers "identify patterns of abuse [...] and assess threats" (Vilk, 2020, n.p.). There should also be protocols in place for responding to phone and email onslaughts, assessing the credibility of threats, as well as a clear public communications plan that does not exacerbate or prolong the abuse of workers. In developing these policies and procedures, administrators are advised to reach

out to other organizations and learn from those who have implemented strong response mechanisms. Importantly, the research suggests that organizations ensure that these policies and protocols are well communicated to workers and efforts are made to fully "socialize" these into the workplace (Schaefer-Ramirez, 2017, p. 91). The second preparatory recommendation made to organizations is to educate and provide appropriate training to their workers (n=65). These types of recommendations emphasize the importance of ensuring that staff are aware of and prepared for the problem of online abuse. This training should equip workers with knowledge of the appropriate precautions to take to protect themselves, and what to do if they or a colleague are attacked.

The second most common recommendation made to organizations is to support workers that experience online abuse. The research frequently advises employers to support targets in the aftermath of an attack by providing access to legal counsel, mental health counseling, and modifying the target's work responsibilities as requested (n=70). Organizations are advised to denounce the abuse publicly and stand in support of their workers when doing so (n=47). Failing to do this can embolden perpetrators and exacerbate the abuse. Other supportive recommendations include taking workers' reports of online abuse seriously, acknowledging the harm of the incident, and not minimizing or dismissing the severity of the event (n=24). In responding to the attack, employers should consult with the target about how they would like to proceed (n=24). Some may welcome further publicizing of the issue and rallying the support of a broader community, while others may prefer to disengage and allow the incident to blow over. Because there is no "one size fits all" model, employers are advised to prioritize the target's needs and respect their wishes. It is also recommended that employers assess the threat level and provide appropriate security measures to ensure the worker's safety (n=21). Like the recommendations made for individual targets, it is recommended that supervisors appoint someone–such as a colleague, the company's social media team, or IT–to take control of the target's email and social media accounts to protect them from abuse and spearhead the task of blocking, reporting, and documenting abuse (n=14).

Various changes can be implemented by organizations to better address the issue of online abuse. Research suggests that if organizations are going to expect and encourage engagement with the public, they need to be more actively involved in monitoring and moderating public discussions and protecting their workers from abuse (n=26). This means creating and maintaining spaces for public deliberation, being aware of the online discussion that their workers are involved in, setting clear expectations for civil discourse for the public, and enforcing those expectations through deleting abuse and blocking abusers. Some documents further emphasize that organizations must consider the ways that online abuse uniquely targets and impacts equity-deserving groups when developing any policies and procedures (n=14). In the case of higher education, a few also point to the need for organizations to reiterate a commitment to academic freedom and implement additional professional protections that can shield knowledge workers from reprimand or termination (n=5). This is particularly relevant when organizations receive pressure to fire workers from external sources. A few times it was identified that these protections, as well as any organizational support provided, need to be extended to contract workers (n=7).

RESULTS

OTHER INSTITUTIONS

Various other players have a role to play in addressing the issue of online abuse. Most prominently, the research identifies governments and policymakers as key actors who have a role to play in addressing online abuse (n=91), which includes calls to reform existing laws (n=13). The role of government, as articulated in the research, is to invest in projects and organizations that combat or research this problem; raise awareness and educate the public about the issue; update regulatory frameworks; establish accountability mechanisms for platform companies; and collaborate internationally to protect democracy and ensure compliance with international human rights law.

After governments and policymakers, social media platform companies need to recognize their responsibility in combating online abuse (n=83). The research recommends more transparency from platforms about their content moderation policies and enforcement practices, and to make improvements to these processes so that violations are dealt with quickly and fairly. Recommendations for platforms also point to the need for more flexible tools for users that help stem the flow of abuse, a simplified process of documenting abuse so that it can be used as evidence in a court of law, and working with civil society organizations to develop tools and policies that are inclusive.

Lastly, law enforcement, prosecutors, and judges are not sufficiently informed on the issue of online abuse. There are repeated calls in the current research for more extensive education and training for these groups, and recommendations for better protocols and best practices to be put in place for investigating and prosecuting incidents (n=29). Other, less frequently mentioned actors include professional associations (n=3); publishers (n=3); and civil society organizations (n=7).

KNOWLEDGE GAPS

Our scoping review also identifies several existing knowledge gaps in the research concerning online abuse. Most prominently, additional studies are needed to improve our understanding of people's experiences with online abuse and the impacts that it has on them, their communities, organizations, and society at large (n=17). There is a need to explore how online abuse is experienced differently across different demographics and subject positions (n=13). There is also a need for additional research that can refine our understanding of the dimensions of the problem (n=12). Less frequently mentioned gaps include research on targets' responses, coping mechanisms, and their effectiveness (n=7); the implications of online abuse for research (n=2); studies of online abuse legislation and policy (n=2); its implications for democracy (n=2); and comparative studies that can understand the way that online abuse operates in different contexts (n=2).

DISCUSSIONS AND IMPLICATIONS

THE COST OF ONLINE ABUSE AND WHO'S FOOTING THE BILL

The recommendations made for individuals show the significant investment of time, energy, and personal resources that knowledge and public education workers are being asked to make to protect themselves from online abuse. Some of the suggested cybersecurity measures, such as investing in quality anti-virus software or signing up for a data scrubber service, cost money. The time and money such recommendations involve must be considered in combination with the negative repercussions that online abuse can have on one's career and professional life, particularly for the precariously employed. Quite literally, online abuse can be expensive.

Cultural critic and founder of Feminist Frequency, Anita Sarkesian (2015), explains that the extra time, energy, and money spent on dealing with online abuse is akin to a "tax" that individual targets are shouldering. Importantly, as Sarkesian (2015) herself notes, this tax is not evenly distributed. It is "levied disproportionately at women, people of color, queer and trans people, and other oppressed groups for daring to express an opinion in public" (n.p.). Given that equit deserving groups are disproportionately targeted for online abuse (see Results section), they must invest more into preparing for or responding to it – an added cost that they are having to bear to participate on par with their white, cis-gendered, heterosexual male colleagues.

This reality points to an important diversity, equity, and inclusion issue. Those footing the bill of online abuse are those who are already most likely to experience oppression and marginalization. In this way, online abuse exacerbates and further entrenches existing social and economic inequities.

Furthermore, the impact that online abuse has on equity-deserving groups must be considered in context of lifelong experiences of oppression and marginalization through systems of sexism, racism, homophobia, ableism, and xenophobia, for example. Compounding this, research shows that the online abuse directed at members of equity-deserving groups is itself sexist, racist, homophobic, ableist, and xenophobic (Duggan, 2017a; 2017b).

Unfortunately, the current research does not speak to the way that this changes the impact online abuse has on diverse subject positions. While it often acknowledges the heightened impact for members of equity-deserving groups, the research in our scoping review did not move beyond this acknowledgment to unpack the nuance of those experiences and their impacts on individual targets and their communities. That said, it stands to reason that the impact of an attack will be qualitatively different for people in marginalized groups. Not only because they are operating in a barren support environment, but because this environment is located within broader systems of oppression.

The costs of online abuse also extend to employers and organizations. As the various individualized responses to online abuse show (see Findings), workers are directing much of their attention towards mitigating abuse, rather than channeling those productive energies into their work. Organizations and institutions can waste valuable resources dealing with the consequences of online abuse by having to respond to social media attacks, address targeted threats, and manage public relations, all of which drain an organization's personnel and financial resources. Put simply, online abuse has severe consequences for diversity and inclusion in the knowledge economy for employers and employees with damaging implications for innovation.

DISCUSSIONS AND IMPLICATIONS

Lastly, the impacts of online abuse also reverberate outwards to produce broader societal harms. It limits who feels comfortable taking up digital space and how they participate online. It affects what work is done and shared with online audiences, what stories are told, which projects are explored, and what policy angles are covered. In other words, it limits the kind of knowledge that is produced. Online abuse functions to push narratives and identities that challenge the status quo to the margins. In doing so, public life suffers because it loses out on diverse and potentially valuable perspectives that can propel public discourse forward.

Ultimately, these impacts combined have serious consequences for innovation because online abuse limits who is "safe" to speak and what is "safe" to speak about.

AN INDIVIDUALIZED PROBLEM

The responses to experiences of online abuse underscore the fact that this burden is largely shouldered by individuals and their networks. Engaging in forms of "anticipatory labour" to prevent abuse; "quietly coping" by trying to ignore the abuse or filter it out with the help of friends; and "fighting back" by challenging perpetrators directly and publicly are all personal survival strategies that betray broader systemic failings. Taken together with the series of ineffectual and sometimes punitive responses from management (see Findings), our findings demonstrate that knowledge workers are operating in a broader context of inadequate institutional and organizational support.

Individuals are bearing the brunt of this problem, in part, because of what we call a pervasive culture of ambiguity that is visible across sectors and occupations. This ambiguity surrounds what employers can, will, and should do about online abuse. Firstly, ambiguity about what organizations can do reflects generalized doubt in employers' capacity to help prevent, protect, or alleviate the impact of abuse on workers.

For instance, one media worker recounted her experience reporting online abuse to her employer:

> ***"They don't care, I've had meetings with HR and with my boss and they've basically been like, 'Beyond physical safety, I don't know what you want us to do.'"*** (Sobieraj, 2020, p. 51).

The notion that employers are unable to help contributes to a culture in which workers try to adopt a "thick skin" for online abuse as an unavoidable reality of their work (Koirala, 2020, p. 53).

Secondly, ambiguity about what the employer will do can be understood as the perception that employers do not view online abuse as an organizational problem and therefore do not feel an obligation to address it. For instance, one woman of color working at a large newspaper explained her decision to not involve management in her experience:

> ***There is a long history of women of color, particularly black women in any corporate environment being seen as difficult for raising issues about race. And I certainly do that already, raise issues about race within our own newsroom. But I feel like if I started adding on more of the things that I face when I'm out in the field on my own... I, first of all, I don't feel like they would feel responsibility for helping with that. And second, I feel like I'm already perceived as difficult*** (Miller, 2020, p. 81).

As the above comments demonstrate, the perception that their employers see online abuse as a personal problem discourages workers from seeking support because they believe reporting it will have no effect or, more troublingly, that it will further exacerbate the negative impacts they experience. The level of responsibility that an

DISCUSSIONS AND IMPLICATIONS

organization owes to its workers as they interact with the public and where that organization's obligation ends are not clearly defined. This worker's experience further speaks to the additional burden that members of equity-deserving groups carry to sustain the "normal" functioning of the workplace and underscores the need for intersectional solutions.

Finally, ambiguity regarding what the organization should do reflects workers' lack of clarity regarding the responsibility that the organization has to its workers, what constitutes abuse, and what warrants reporting as a workplace issue.

As one female journalist explained,

> ***Nobody has ever talked about it [any sort of abuse]. We [female journalists] still hesitate to report it to our boss if we are harassed physically. So, reporting online harassment might be ridiculed. Many of us are not even sure what extent of harassment is bearable and what should be reported... Organisational policies on such issues would have helped but we don't have one that deals with cyber-attacks*** (Koirala, 2020, p. 54).

This ambiguity around what "counts" as abuse and what is serious enough to report discourages targets from coming forward and contributes to fears that experiences won't be taken seriously by management. In conversation with The Walrus, Tracy Porteous, executive director of the Ending Violence Association of BC, explains

> ***'Its kind of like death by a thousand flashes.' [...] One incident feels too dramatic to raise and so goes unmentioned. And then so does the next."*** (McCabe, 2021, n.p.)

This hesitancy to report is likely exacerbated for freelancers and contract workers, who operate at a distance from the organizations that employ them and may feel that their employer's obligation to them is lessened as a result. They may also be additionally reluctant to bring problems to their temporary employers for fear that doing so will put future contracts in jeopardy. In short, precariously employed workers have more to lose by reporting incidents to their employers.

Ultimately, this "culture of ambiguity" leaves the responsibility for support and protection with the individual. These examples also underscore that any implemented policies, reporting mechanisms, or other protocols must take a gender and race-sensitive approach. In developing these, employers must consider how different identities and lived experiences will provide different frameworks through which online abuse is experienced and understood, and that will inform how different workers choose to respond and what support mechanisms they require.

LEAKY SAFETY NET

Self-reliance is an understandable response when operating in a context of limited or no support. While individuals are encouraged to report abuse to their supervisor, our research shows that their employers and other formal institutions have repeatedly fallen short in responding to abuse and offering support and protection (see Findings). For example, recommendations in the research encourage targets to involve law enforcement (n=35). However, that same research underscores that law enforcement needs to be educated on this issue and trained on how to effectively deal with complaints of online abuse (n=29). This recommendation emerges from the experiences of targets who, upon reporting an incident of online abuse, found themselves in a position to

DISCUSSIONS AND IMPLICATIONS

have to educate officers on particular social media platforms, on the significance of these spaces to their work, and the severity of the abuse. It is not uncommon for victims to have their concerns dismissed, or to be told to turn off their computers. Furthermore, such advice is unhelpful in the context of systemic racism. Police support is not equally available to those who face systemic (and outright) racism and discrimination and do not see the police as an institution that can help (Goel et al., 2017). Additionally, while individuals are frequently advised to report abuse to the platform (n=41), the research also contains the common critique that platforms have inconsistent, opaque, and lax enforcement practices. Recommendations to improve the transparency and effectiveness of platform content moderation procedures were prevalent in the research (n=83).

Taken together, these recommendations result in passing the buck; none of it is helpful, and individuals are left holding the bag.

OUR RECOMMENDATIONS

The research shows that targets are already doing what they can. However, effectively tackling the issue of online abuse will require a more robust approach whereby institutions acknowledge the important role that they have to play in preventing online abuse and supporting the workers who become targets. As such, we developed 8 practical steps for employers to implement.

1. **Proactive and supportive policies**
   The work of protecting and supporting knowledge workers from online abuse must begin before an incident occurs. At a minimum, this involves having clear and supportive policies and procedures in place and taking steps to ensure that these are well-socialized into the workplace culture.

   Develop a plan that considers the following:
   a. What forms of communication should be reported to a supervisor?
   b. How should workers report an experience of abuse?
   c. What processes will be set in motion when an incident is reported?
   d. What support will be provided to targets of online abuse?
   e. Will protections, supports, and resources be extended to contract workers? If so, will they be offered beyond the duration of their contract? For how long?

2. **Change the workplace culture**
   The larger task is to cultivate a workplace culture where workers feel empowered to report, believe that they will be taken seriously, and know that they will be supported when they do so.
   While training and education for workers may help minimize the number of incidents, training for managers, supervisors, and administrators is also critical.

   Training should include:
   a. A comprehensive overview of what online abuse is, where it occurs, and what it looks like.
   b. Education around the individual impacts of online abuse. This would include dispelling the belief that online abuse happens “just online.”
   c. Understanding how online abuse disproportionately targets women, BIPOC, and LGBTQIA+ individuals.

   These are basic steps, but they are important in transforming a workplace culture into a strong support environment by redistributing the onus of responsibility from individual workers to the broader organization.

DISCUSSIONS AND IMPLICATIONS

3. **A gender and race-sensitive approach to policies and procedures is critical**
Any implemented policies, reporting mechanisms, or other protocols must take a gender and race-sensitive approach. In developing these, employers must consider how different identities and lived experiences will provide different frameworks through which online abuse is experienced and understood. This will inform how different workers choose to respond to an experience of online abuse, how much trust they have in organizations to help, and what truly supportive mechanisms will look like given these different subject positions.

4. **Expand the office walls**
Employers should consider rethinking what constitutes the workplace and a workplace incident. This is especially necessary if workers are expected (either explicitly or implicitly) to engage with the public online and use DCTs in the course of their work.

5. **Take your lead from targets**
There is no "one size fits all" solution for dealing with online abuse. An experience can have very different impacts on different workers. It is important to have procedures and supports that are flexible and that prioritize the needs of each target. While some may welcome the opportunity to respond to the incident and rally the support of a broader community, others may prefer to let the event blow over. Take your lead from targets.

6. **Responding publicly: Don't panic, condemn the abuse, and stand behind your workers**
Responding publicly to an incident of online abuse is a delicate matter. In the past, organizations have responded to public pressure in ways that have emboldened perpetrators and exacerbated the abuse that the worker experiences (Campbell, 2018; Grollman, 2015). There are some simple steps to follow to avoid making the same mistakes. If you become aware that a worker has become the target of an attack, or if your office suddenly comes under a swell of public pressure to dismiss or punish someone in your employ:

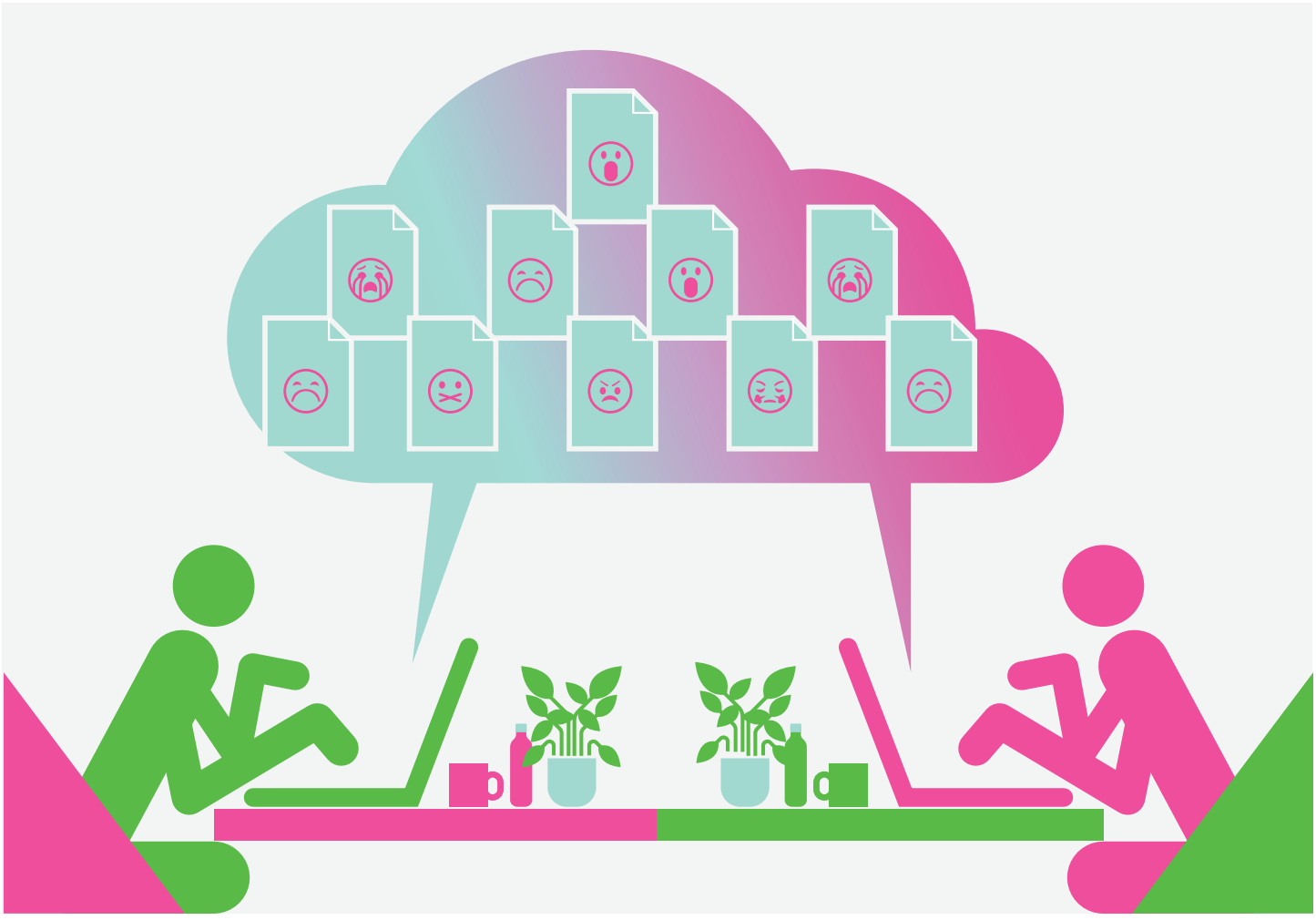
a. Do not release a statement, promise anything to members of the public, or take any action at all without first speaking with the target to better understand the situation.

b. Publicly and explicitly condemn any abuse. Make it clear that harassing behavior contradicts the values of your organization and that you will not tolerate the abuse of your employees.
c. Publicly express your support for the target and their work.

7. **Unions and professional associations: Begin the conversation**
The scoping review retrieved very little literature from unions and/or professional associations that provide information, advice, or resources for workers across industries. This is somewhat surprising given the impact that online abuse has on how knowledge workers conduct and share their work. These organizations are also well-positioned to pressure employers to improve procedures and expand the cadre of support available for targets. We recommend that these organizations create spaces of dialogue to have conversations about online abuse and how it uniquely impacts those within their fields. These groups could organize workshops, conferences, develop resources, and advocate for improved standards within their industry.

DISCUSSIONS AND IMPLICATIONS

8. **Pressure governments to do more to combat this problem**
Unions and employers alike can lobby governments to do more to prevent online abuse. Governments can help to reduce the damage of this problem by investing in projects and organizations that combat or research this problem; raising awareness and educating the public about the issue; updating regulatory frameworks; establishing accountability mechanisms for platform companies; and, collaborating internationally to protect democracy and ensuring compliance with international human rights law.



DISCUSSIONS AND IMPLICATIONS

CONCLUSIONS AND FUTURE RESEARCH

SUMMARY OF FINDINGS

The current academic and grey literature proposes a host of recommendations that can help to protect and support knowledge workers. These recommendations identify a series of different stakeholders who have a role to play in combating online abuse, which includes individual targets, their friends, families and peers, employers, governments, platform companies, and law enforcement. Recommendations made for individuals prioritize limiting their vulnerability and minimizing the damage that an attack might have. Friends, families, and peers are positioned in a support role and are advised to offer help in whatever ways they can. For employers, the recommendation is to be proactive in setting up appropriate policies and procedures and socializing these into the workplace community. Governments are also identified as having a key role, particularly in their capacity to offer funding, improve awareness, and provide regulatory frameworks and accountability mechanisms. The recommendations for platform companies are to improve moderation policies and procedures and increase transparency in how they operate. Finally, the research recommends that law enforcement officials undergo more training to effectively respond to complaints of online abuse. These diverse recommendations reflect the complexity of this problem and the fact that solutions will require a cooperative, multifaceted approach.

While the task ahead is challenging, the consequences for failing to grapple with this are significant for worker engagement, productivity, and the capacity to innovate. As we have explained above, the individualized ways that workers are coping with online abuse demands a significant investment of time and energy that detracts from their capacity to do their work. The emotional toll that these experiences take also causes workers to stop using DCTs, self-censor, and generally engage less in the discussions of their industry.

This tendency to retreat in the face of online abuse is more troubling when we understand that equity deserving groups are most likely to experience abuse, and thus most likely to withdraw at significant personal, professional, and societal costs. In effect, the consequence of online abuse is to limit the plurality of voices and diversity of perspectives that is available in the public sphere.

FUTURE RESEARCH

This scoping review has revealed several important areas for future research. Firstly, while the research frequently acknowledged that the experience of online abuse was more prevalent for members of equity deserving groups and that this abuse often targeted the person's race, gender, sexual orientation, etc., research that investigates what relationship this has to the impact that online abuse has was absent. Future research questions related to this include: what harms emerge when one's identity is the raison d'etre for abuse, and how do those harmsdiffer across subject positions? How do these impacts inform how people choose to respond to an attack, and with what outcomes for participatory parity in the digital knowledge economy?

Secondly, although we hoped to capture the efficacy of different implemented approaches, the research did not include such analysis. While there is a breadth of research that speaks to the harms of online abuse, little research exists (to the best of our knowledge) that examines how successful certain responses have been in addressing abuse and supporting workers (for an example that does, see Blackwell et al., 2017). It seems efficacy has yet to be widely measured. In addition to more resources, support, and protection for workers, we need ways of knowing

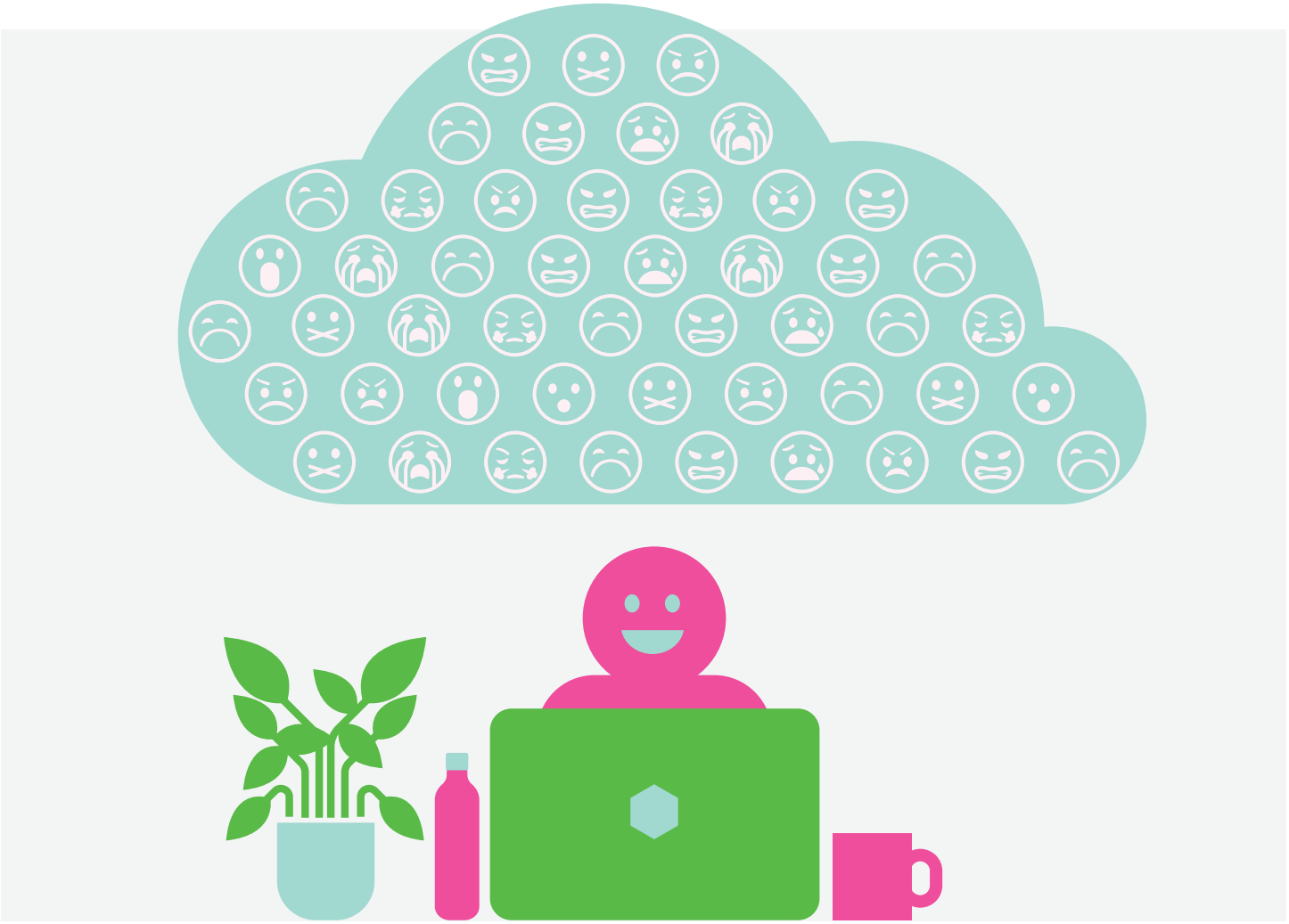
DISCUSSIONS AND IMPLICATIONS

whether these instruments produce their intended effect. Are they working? Are they actually helpful?

Thirdly, additional research is needed on the impact of witnessing online abuse. Most of the research examined in this study considers the impact of online abuse on targets, however, little is known about how witnessing an incident impacts the behavior of bystanders. Such work could reveal that the impacts of online abuse are happening on a much larger scale than is currently understood and measured.

Finally, research that investigates the experiences of online abuse among the precariously employed is necessary. While some texts examined here underscored how freelancers and contractors are uniquely vulnerable to experiencing online abuse, and that it has particularly damaging impacts for this group, this research did not include a single study that centered on the experiences of those workers, explicitly.

This report provides a comprehensive overview of existing research related to protection from, support for, and an understanding of the impacts of online abuse for knowledge workers. Based on this research, we created 8 recommendations that organizations can implement to create a stronger support landscape and reduce the adverse impacts of online abuse to create a safer and more equitable digital knowledge economy.



BIBLIOGRAPHY

Amnesty International. (2018). Violence Against Women Online in 2018. Amnesty International. https://www.amnesty.org/en/latest/research/2018/12/rights-today-2018-violence-against-women-online/

Anderson, S., Allen, P., Peckham, S., Goodwin, N. (2008). Asking the right questions: scoping studies in the commissioning of research on the organization and delivery of health services. Health Res Policy Sys, 6. 7-10.

Angus Reid. (2016). Trolls and tribulations: One-in-four Canadians say they're being harassed on social media. Angus Reid Institute. https://angusreid.org/social-media/

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. International journal of social research methodology, 8(1), 19-32.

Blackwell, Lindsay., Diamond, Jill., Schoenebeck, Sarita., and Lampe, Cliff. (2017). Classification and its consequences for online harassment: Design insights and HeartMob. Human-Computer Interaction, 1(CSCW), article 24, 1-19.

Brinkley, I.(2006). Defining the knowledge economy: Knowledge economy programme report. The Work Foundation.
https://www.knowledge4all.com/Temp/Files/9219fc8b-7263-416d-b3dc-a7dca118761f.pdf

Campbell, C. (2018). AreNanet 'folded like a cheap card table' says fired Guild Wars 2 writer. Polygon.
https://www.polygon.com/2018/7/9/17549492/arenanet-jessica-price-guild-wars-2-writer-fired

Cassidy W, Faucher C and Jackson M (2014) The dark side of the ivory tower: cyberbullying of university faculty and teaching personnel. Alberta Journal of Educational Research 60(2): 279–299.

Chadha, K., Steiner, L., Vitak, J., and Ashktorab, Z. (2020). Women's Responses to Online Harassment. International Journal of Communication, 14, 239-257.

Citron, D.K. (2014). Hate crimes in cyberspace. Harvard University Press.
Crear-Perry, J. (2018). Race isn't a risk factor in maternal health: Racism is. Rewire News Group.
https://rewirenewsgroup.com/article/2018/04/11/maternal-health-replace-race-with-racism/

Desilver, D. (2021). Q & A: What we've learned about online harassment. Pew Research Center.
https://www.pewresearch.org/fact-tank/2021/01/13/qa-what-weve-learned-about-online-harassment/

BIBLIOGRAPHY

Duggan, M. (2017a). 1 in 4 Black Americans have faced online harassment because of their race or ethnicity. Pew Research Center.
https://www.pewresearch.org/fact-tank/2017/07/25/1-in-4-black-americans-have-faced-online-harassment-because-of-their-race-or-ethnicity/

Duggan, M. (2017b). Online harassment. Pew Research Center.
http://www.pewinternet.org/2017/07/11/online-harassment-2017/

Duggan, M. (2014) Online harassment. Pew Research Center.
http://www.pewinternet.org/2014/10/22/online-harassment/

Eckert, S., and Metzger-Riftkin, J. (2020). Doxxing, privacy and gendered harassment: The shock and normalization of veillance cultures. M&K Medien & Kommunikationswissenschaft. 68(3), 273-287.

Elmer, G., Burton, A.G., and Neville, S.J. (2020). Zoom-bombings disrupt online events with racist and misogynist attacks. The Conversation.
https://theconversation.com/zoom-bombings-disrupt-online-events-with-racist-and-misogynist-attacks-138389

Ferber, A. (2018). "Are You Willing to Die for This Work?" Public Targeted Online Harassment in Higher Education: SWS Presidential Address. Gender & Society, 23(3), 301-322.

Goel, S., Perelman, M., Shroff, R., and Sklansky, D.A. (2017). Combatting police discrimination in the age of big data. New Criminal Law Review, 20(2), 181-232.

Gosse, C. (2021), ""Not the real world": Exploring experiences of online abuse, digital dualism, and ontological labor." In: Bailey, J., Flynn, A. and Henry, N. (Ed.) The Emerald International Handbook of Technology Facilitated Violence and Abuse. Bingley, UK: Emerald Publishing Ltd. pp. 47-64.

Gosse, C. and Burkell, J. (2020). Politics and porn: how news media characterizes problems presented by deepfakes. Critical Studies in Media Communication, 37(5), 497-511.

Gosse, C., Veletsianos, G., Hodson, J., Houlden, S., Dousay, T., Lowenthal, P., & Hall, N. C. (2021). The hidden costs of connectivity: Nature and effects of scholars' online harassment. Learning, Media, and Technology, 46(3), 264-280.

Grollman, E.A. (2015). Scholars under attack. Inside Higher Ed.
https://www.insidehighered.com/advice/2015/07/09/essay-how-support-scholars-under-attack

Haque, Z. (2018). How the gig economy is widening racial inequality. NewStatesman.
https://www.newstatesman.com/politics/economy/2018/02/how-gig-economy-widening-racial-inequality

BIBLIOGRAPHY

Hodson, J., Gosse, C., and Veletsianos, G.,(2021).
Analog policies in a digital world: How workplace harassment policies need to adapt to an increasingly digital education environment Academic Matters.
https://academicmatters.ca/analog-policies-in-a-digital-world-how-workplace-harassment-policies-need-to-adapt-to-an-increasingly-digital-education-environment/

Hodson, J., Gosse, C., Veletsianos, G., and Houlden, S. (2018).
I Get By With a Little Help From my Friends: The Ecological Model and Support for Women Scholars Experiencing Online Harassment. First Monday, 23(8), n.p

Houlden, S., Hodson, J., Veletsianos, G., Gosse, C., Lowenthal, P., Dousay, T., and Hall, N. (2021).
Support for Scholars Coping with Online Harassment: An Ecological Framework.
Feminist Media Studies. n.p.

Jane, E. (2014).
Back to the kitchen, cunt: Speaking the unspeakable about online misogyny.
Continuum, 28(4), 558-570.

Koirala, S. (2020).
Female journalists' experiences with online harassment: A case study of Nepal.
Media and Communication. 8(1), pp. 47-56.

Lenhart, Amanda., Ybarra, Michele., Zickuhr, Kathryn., and Price-Feeney, Myeshia. (2016).
Online harassment, digital abuse, and cyberstalking in America.
Data & Society Research Institute and Center for Innovative Public Health Research Report.
https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

Levac, D., Colquhoun, H., & O'Brien, K. K. (2010).
Scoping studies: advancing the methodology.
Implementation science, 5(1), 1-9.

Massanari, A. (2017).
#Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. New Media and Society, 19(3), 329-346.

McCabe, S. (2021).
Workplace harassment goes digital. The Walrus.
https://thewalrus.ca/workplace-harassment-goes-virtual/

McGlynn, C. and Rackley, E. (2017a).
Beyond 'revenge porn': The continuum of image based sexual abuse. Feminist Legal Studies, 25, 25-46.

BIBLIOGRAPHY

McGlynn, C. and Rackley, E. (2017b).
Why 'upskirtting' needs to be made a sex crime. The Conversation.
https://theconversation.com/why-upskirting-needs-to-be-made-a-sex-crime-82357

Melovic, B., Stojanovic, A.J., Vulic, T.B., Dudic, B., Benova, E. (2020). Int. J. Environ. Res. Public Health, 17(16), 5816.

Milano, B. (2021).
With Covid spread, 'racism — not race — is the risk factor. The Harvard Gazette.
https://news.harvard.edu/gazette/story/2021/04/with-covid-spread-racism-not-race-is-the-risk-factor/

Miller, K. C. (2020).
Harassing the fourth estate: The prevalence and effects of outsider-initiated harassment towards journalists. [Doctoral dissertation, University of Oregon]. Scholars Bank, University of Oregon.
https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/25638/Miller_oregon_0171A_12757.pdf?sequence=1&isAllowed=y

Online SOS. (2020).
Threats of violence: Responses and considerations for journalists facing threats of violence online.
https://onlinesos.org/content/3-resources/3-action-center/6-online-threats-of-violence/threats-of-violence-action-plan.pdf

Peters, M. D., Godfrey, C. M., Khalil, H., McInerney, P., Parker, D., & Soares, C. B. (2015).
Guidance for conducting systematic scoping reviews. JBI Evidence Implementation, 13(3), 141-146.

Ross, A. (2020).
Death threats aimed at Dr. Bonnie Henry mirror contempt faced by female leaders, experts say. CBC.
https://www.cbc.ca/news/canada/british-columbia/dr-bonnie-henry-women-leaders-death-threats-1.5736198

Sarkesian, A. (2015, December 5).
Speak up & stay safe(r): A guide to protecting yourself from online harassment. Feminist Frequency.
https://feministfrequency.com/2015/12/08/speak-up-stay-safer-a-guide-to-protecting-yourself-from -online-harassment/

Schaefer-Ramirez, V. A. (2017).
Cyber-harassment in higher education: A study of institutional policies and procedures.
[Doctoral dissertation, Pepperdine University]. ProQuest DissertationPublishing

Slupska, J. and Tanczer, L.M. (2021)
Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things. In: Bailey, J., Flynn, A. and Henry, N. (Ed.) The Emerald International Handbook of Technology Facilitated Violence and Abuse. Bingley, UK: Emerald Publishing Ltd. pp. 663-688.

BIBLIOGRAPHY

Sobieraj, S. (2020).
Credible Threat: Attacks Against Women and the Future of Democracy.
New York, NY: Oxford University Press.

Stein, A. & Daniels, J. (2017).
Going Public: A Guide for Social Scientists.Chicago, IL: University of Chicago Press.

Traer S., Bednar P. (2021)
Motives behind DDoS sttacks. In: Metallo C., Ferrara M., Lazazzara A., Za S. (eds) Digital Transformation and Human Behavior. Cham, Switzerland: Springer

Veletsianos, G., Houlden, S., Hodson, J., and Gosse, C. (2018).
Women Scholars' Experiences with Online Harassment and Abuse: Self-protection, resistance, acceptance, and self-blame. New Media and Society, 20(12), 4689-4708.

Vilk, V. (2020).
What to do when your employee is harassed online. Harvard Business Review.
https://hbr.org/2020/07/what-to-do-when-your-employee-is-harassed-online

Vogels, E.A. (2021).
The state of online harassment. Pew Research Center.
https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf

Wallis, C. (2020).
Why racism, not race, is a risk factor for dying of Covid-19. Scientific American.
https://www.scientificamerican.com/article/why-racism-not-race-is-a-risk-factor-for-dying-of-covid-191/

APPENDICES

FURTHER RESOURCES TO EXPLORE

- HeartMob
- Online Violence Response Hub
- TrollBusters
- The eQuality Project
- Crash Override: Automated Cybersecurity Helper
- Electronic Frontier Foundation: Cybersecurity Tools
- Global Forum for Media Development: Guide to Prevent Zoombombing
- Citizen Lab: Security Planner
- Access Now Digital Security Helpline
- Tactical Tech: Training Curriculum
- Hate Campaigns - What You Should Do: by Suomen Journalistiliitto, Finlands Journalistförbund

Layout + Design by Simon Paul