TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN: TAKING STOCK OF EVIDENCE AND DATA COLLECTION

Contents

Introduction

A central tension of the digital revolution and the uptake of online information and communications technologies (ICTs) is its potential for both positive and negative gendered impacts, as technology "mirrors the societies that create it."[1] On the one hand, online spaces and digital tools can facilitate access to essential information and services, unleashing educational and employment opportunities for women and girls.[2] They can be leveraged to organize movements, including around gender equality and gender justice.[3] Beyond their potential to enable greater social, economic or political agency, ICTs can also play a valuable role in fostering creativity, community and leisure for women and girls.[4]

On the other hand – and while the gender digital divide prevents vast portions of women and girls from enjoying these potential benefits – for those who *are* online and *do* have access, a growing body of evidence sheds light on the ways in which the digital revolution has exacerbated existing, and even created new, forms of gendered inequalities and oppression.[5]

Indeed, as feminists and women's movements have been contending for some time now,[6] various digital tools and modalities are inextricably linked to the offline world, exacerbating its inequalities and power relations.[7] In other words, the design of, governance and control over, and access to this world and its tools still overwhelmingly favours men and largely excludes the perspectives, experiences and needs of women, girls and gender minorities.[8]

In an increasingly digitized world, one of the more concerning dynamics is violence against women (VAW) that is committed, assisted, aggravated or amplified by the use ICTs or other digital tools.[9] In recent years, particularly amid a protracted pandemic that further shifted peoples' lives online, technology-facilitated violence against women (TF VAW) has commanded attention from scholars, digital rights advocates, women's rights movements, VAW service-providers and others keen to understand and gage its scale (see Box 1). Much of this research has been used to advocate for responses from governments and the technology sector, among others.[10]

Box 1.
Emerging consensus around a definition of technology-facilitated violence against women

Until recently, the international community lacked a shared definition of TF VAW, which has been one of the foremost challenges to collecting data and producing comparable research on this type of gender-based violence. Recognizing this key barrier **while** developing this paper, UN Women convened diverse global experts to develop a shared definition. The resulting definition builds on work from academics, governments, national statistical offices, feminist movements, international organizations and other gender equality advocates:[11] **Technology-facilitated violence against women is any act that is committed, assisted, aggravated or amplified by the use of ICTs or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms.**

In this definition, 'ICT' is an umbrella term that includes mobile phones, the Internet, social media platforms, computer games, text messaging, email and other related technologies. Aligned with guidance from the Special Rapporteur on violence against women and girls, its causes and consequences, this definition uses the term 'women' to include girls, whenever applicable, recognizing that young women and girls are often targets of technology-facilitated violence.[12] Like all other forms of VAW, TF VAW is rooted in and enabled by discriminatory gender norms that intersect with other forms of discrimination based on race, ethnicity, gender identity, sexual orientation and ability, among other factors.

This definition also acknowledges that perpetrators

>>

of TF VAW use a variety of technology-based tactics to enact harm. Some of these are unique to digital contexts, including: doxing, gender trolling, hacking, cybergrooming, using fake accounts and image-based abuse. TF VAW also includes behaviours that are *not* unique to digital contexts, including: harassment, stalking and exploitation, but may be assisted, aggravated or amplified by the use of ICTs or other digital tools.[13] Crucially, this framing acknowledges that while TF VAW has its own distinct features, it is "part of the continuum of multiple, recurring and interrelated forms of gender-based violence."[14]

Note: While UN Women and WHO employ the term TF VAW, others may refer to technology-facilitated gender-based violence, but the common definition describing the phenomenon remains the same.

While technology-facilitated violence has an extensive reach, women and girls are disproportionately impacted.[15] Available evidence suggests that women are more likely to be targeted because of their sex and gender identity, to experience more severe forms, and are also more likely to face serious and longer-lasting negative impacts.[16] For example, TF VAW is often directly linked to offline violence[17] and women often change the way they use (or opt out of using) ICTs due to associated risks.[18] In these ways, TF VAW exacerbates the gender digital divide, undercuts access to information and services, and infringes upon women's rights to participate in public life.[19] Beyond these more direct negative impacts on women, a growing body of research illustrates the ways in which TF VAW amplifies and normalizes existing cultures of patriarchal violence and misogyny, while enabling the emergence of new ones.[20]

Despite a growing evidence base and accelerated efforts to develop fit-for-purpose quantitative and qualitative research and data collection methods, significant gaps remain in our understanding of the scale and particular manifestations of TF VAW — including how women who face intersecting forms of discrimination experience or resist it. Such data gaps stymie the efforts of policymakers and service-providers keen to develop evidence-driven strategies to prevent and respond to TF VAW. While safely collecting data on VAW — offline or online — is always rife with methodological, ethical and sociopolitical considerations,[21] TF VAW presents distinct additional difficulties. These include lack of consensus on what counts as technology-facilitated violence, the multi-stakeholder and transborder nature of the online world, and concerns around privacy and protection, among other challenges.[22] In a context where a lack of data can become rationale for inaction,[23] continued consensus-building across the international community to develop shared definitions, indicators and promising practices for collecting data on TF VAW is both a pressing challenge and an opportunity.

Drawing on a phased scoping review[24] of academic and grey literature,[25] this paper offers a landscape scan highlighting *what* is known about TF VAW, *who* is currently generating this knowledge and *how* the evidence is being produced. The paper also highlights some of the related ethical and sociopolitical challenges to collecting TF VAW data. As a way forward, actions for strengthening knowledge generation and data collection are proposed, including recommendations on methods and further research.

Approaches to collecting data on TF VAW

This paper looks at quantitative and qualitative data generated by different stakeholders using various methodologies. This includes: **survey data** generated through household and online surveys; **administrative data,** also known as service-based, programmatic or reporting data; **qualitative data**, generated through traditional methods, like key informant interviews and focus group discussions, as well as newer methods, like digital ethnographies; and data generated through **mixed-methods**, such as the use of machine learning to scrape and analyse social media data.

SURVEY DATA

Household surveys are commonly used to collect VAW data, including to estimate prevalence by government agencies, particularly national statistical offices (NSOs), civil society organizations (CSOs) and academics. One key limitation of these surveys is that there are a finite number of questions that can be included, due to resource constraints and respect for participants' time. This poses a challenge for the study of TF VAW, given the many different forms of technology-facilitated violence.

Representative survey data

Specialized VAW studies

Population-based prevalence data produced by NSOs, women machineries or other relevant sectors (mostly via household surveys[26]) are the backbone of many countries' national VAW response policies and programmes. These surveys are usually conducted by women highly trained in survivor-centred approaches for research on VAW[27] and usually only survey adult women. The data, sometimes referred to as "official statistics",[28] are critical for developing prevalence estimates and monitoring states' progress on protecting women's rights to a life free from violence.[29]

Many of these surveys, particularly in low- and middle-income countries, are adaptations of the Domestic Violence Module from the Demographic and Health Survey (DHS) Programme[30] or the World Health Organization (WHO)'s Multi-Country Study. Until

recently, neither of these included questions specific to technology-facilitated violence.[31] While it is promising that more recent NSO-led VAW studies are now including questions related to technology-facilitated violence, these additional questions reflect limited conceptualizations of TF VAW, resulting in a limited understanding of its reach and impacts on different groups of women. More specifically, the reviewed national VAW studies provide quantitative data on the following forms of TF VAW (note that three of the seven reports neither explicitly named TF VAW, nor used related umbrella terms):

→ **Controlling behaviours**: The *Guyana Women's Health and Life Experiences Report* 2018, for example, found that of the 58 per cent of women who reported at least one controlling behaviour from a partner in their lifetime, 13 per cent reported that their partners checked their cell phone to see who they called/who called them.

→ **Stalking**: Georgia's *National Study on Violence Against Women* 2018 found that the most common forms of stalking were "offensive or threatening text messages or emails (2 per cent of all women respondents), loitering or being followed (1 per cent), and offensive, threatening or silent phone calls (1 per cent)."

→ **Sexual harassment**: The Albanian Institute of Statistics' *National Population Survey on VAW* 2019 found that 1.4 per cent of adult women respondents had received or been shown, by someone who is not their husband or boyfriend, sexually explicit or pornographic pictures, photos or GIFs that made them feel uncomfortable, embarrassed or offended.

As illustrated by these examples, the reviewed studies feature some variation in timeframes (some ask for lifetime prevalence, while others specify the last 12 months), and relationship to perpetrators (some ask whether the incident was from a partner or non-partner). Notably, many do not present disaggregated findings by variables that would be useful for intersectional analysis, including age, race and ethnicity, and dis/ability.

Box 2.
Promising practices: Expanding definitions of TF VAW in nation-wide household surveys

The Uganda Bureau of Statistics' 2020 survey on VAW, which was supported by UN Women, illustrates a promising approach to analysing the role of technology in VAW. While most of the reviewed national VAW surveys limit their conceptualization of TF VAW to the use of ICTs to control, stalk or sexually harass, this study also included questions regarding hate speech, finding that about 1 in 5 women in Uganda had experienced "hate speech, meaning language that degrades, insults, threatens or targets someone based on their gender and/or other traits (such as disability, tribe, religion)."

Data were also disaggregated by several socio-demographic variables, allowing for an intersectional analysis of **findings.**[i] For example, women in rural areas were more likely to report online harassment than women in urban areas, specifically in the form of receiving unwanted images and being targeted by gender-motivated hate speech. On the other hand, the study found that urban women were more likely to report receiving offensive advances on social media platforms. The report also highlighted that younger women (aged 18–30) were twice as likely to be harassed as older respondents. Notably, the study found little variation in experiences of online harassment by income status.[ii]

Source: Uganda Bureau of Statistics (UBOS). 2021. "Uganda Violence Against Women and Girls Survey 2020." New York: UN Women.

Specialized ICT studies

Some countries have also begun developing population-based surveys directly on the use and impact of different ICTs and digital tools. Because these surveys are dedicated *specifically* to understanding trends related to ICTs, rather than *all* forms of VAW, they can capture a broader range of TF VAW, and include questions on frequency, impacts, perpetrators and other useful data points. For example, Mexico's National Institute on Statistics and Geography regularly conducts a household survey among men and women, boys and girls aged 12+ with Internet access, to monitor the prevalence of *ciberacoso* (cyberharassment). The latest survey (2021) asks about 13 different "situations" of violence, with data disaggregated by sex, age and education level.[32] Likewise, the Canadian Internet Use Survey asks respondents aged 15+ questions on a number of behaviours that occur online, including bullying, harassment, discrimination and misuse of personal pictures, videos or other content.[33] In comparison, most of the reviewed VAW studies only include a few (1–3) questions on TF VAW, which are generally about the frequency with which cell phones, email and social media are used to control, stalk, monitor or sexually harass.

Because VAW surveys generally only include adult women respondents, this also limits their ability to capture gendered differences in experiences. In contrast, by including both men and women, Mexico's study shows that although women and men reported similar levels of cyberharassment (22.8 per cent and 20.6 per cent, respectively), women were more likely to report gendered forms of harassment. The most commonly reported "situation" for both men and women was "contact through false identities" and "offensive messages" – but women were more likely to report sexual harassment, such as "sexual advances or propositions" (32.3 per cent of women) and "receiving sexual content" (32.1 per cent of women).

However, ICT surveys also have some important limitations. Notably, implementers may be less likely to have specialized training in survivor-centred approaches, given that the focus of ICT surveys isn't *necessarily* VAW, therefore issues such as how to provide referrals to support services for survivors when needed, among other, may not be addressed during enumerators' trainings. Enumerators may include a mix of men and women, which may reduce the likelihood of women survivors or targets of TF VAW reporting sensitive experiences.[34] Lastly, in resource-constrained contexts, developing a separate ICT specific survey, in *addition* to regular VAW surveys, has financing implications.

Specialized TF VAW surveys

This paper identified several dedicated TF VAW surveys that are also population-based and led by non-state organizations, including: the Economist Intelligence Unit, Pew Research Center, Australia's National Research Organisation for Women's Safety (ANROWS) and UN Women. Each of these organizations used online surveys to understand the scope of TF VAW

as well as to generate other actionable insights into its nature, drivers and impacts.[35] Compared to state-led ICT or VAW studies, these surveys offer a unique opportunity to more deeply investigate the many dimensions of TF VAW with the advantage of having an entire dedicated survey. However, the surveys identified here use different definitions and methodologies for collecting and analysing these data, including different denominators, therefore affecting the representativeness of the data. Most focus on studying *online* violence specifically, rather than a broader range of technology-facilitated forms of violence, such as doxing, hacking or image-based abuse. Lastly, while the Pew Research Center, ANROWS and UN Women's surveys include men and women respondents (with Internet access, given their online nature) and are therefore able to identify and compare the prevalence of technology-facilitated violence by gender, the Economist Intelligence Unit's study only included women respondents (again, with Internet access).

Particularly in contexts with greater Internet access, online surveys are useful for collecting large data samples in a short amount of time, including previously overlooked voices. However, as mentioned by the authors of these select reports,[36] they also have notable limitations: Women who share devices, or who lack ownership or control over their device may not be able to respond without jeopardizing their safety and privacy (for example, if they fear an abuser may see their responses). This may both put women at greater risk of violence and it may also affect the validity of the data, as respondents may not report the violence for fear of further violence from the perpetrator. Other limitations include the fact that it may not always be possible to verify that the intended respondent is indeed the person completing the survey, and the fact that assuring the quality of the survey is more challenging generally. The prevalent use of online surveys across all studies reviewed for this paper, indeed, illustrates assumptions that targets or victims of TF VAW are online. Yet, evidence shows that women are leaving online spaces precisely because of experiences or fears of violence.[37] Furthermore, targets of TF VAW are at times offline and unaware of the incident of violence (for example, one's image could be used without consent and shared online, without the target being online or aware of the incident).

Despite these limitations, the more experimental and specialized nature of these studies makes them highly useful (provided the methodological, ethical and safety considerations described above are addressed) for informing the development of data-collection instruments, filling data gaps in official statistics and elucidating the scope of TF VAW – even if their understanding of what TF VAW precisely entails, may vary.

Other representative surveys, with questions on TF VAW

This paper also identified several studies that are neither specific to VAW, ICTs nor TF VAW. For example, the European Union Agency for Fundamental Rights' (FRA) has several population-based surveys that also capture data on TF VAW, such as its LGBTI II survey,[38] as well as its Minority and Discrimination survey.[39] These surveys both ask respondents if they've experienced particular forms of harassment (in the last 5 years and the last 12 months), including being sent offensive or threatening emails or SMS messages and having offensive or threatening comments published on the Internet. Despite being developed and implemented by the same agency, these studies illustrate notable differences in the way data are reported: The Minority and Discrimination survey report includes an analysis of each specific tactic of cyberharassment, while the LGBTI II survey only reports cyberharassment in general. While the LGBTI II survey analyses harassment that respondents perceive as being *because* of someone's gender identity, gender expression, sexual orientation or sex characteristics, and also forms of harassment that occur for "any reason", the Minority and Discrimination survey only measures incidents perceived as being based on one's ethnicity or migration context.

Non-representative survey data

Given the greater costs associated with designing and implementing population-based surveys, it should come as no surprise that much of the identified evidence is drawn from surveys with *non*-representative samples. Such studies were designed and implemented by academic researchers, CSOs[40] and international agencies like UNESCO and UN Women,[41] primarily via online survey instruments (with some exceptions[42]). On the one hand, studies that use convenience sampling may be considered less 'rigorous' or biased. For example, CSO studies with individuals using their services may be less representative of the broader population's experiences, resulting in less generalizable findings.[43] On the other hand, the nimble nature of

these often lower-cost studies is highly valuable for advocacy and programme design. At the onset of the COVID-19 pandemic, for instance, organizations like UN Women, Glitch UK and the End Violence Against Women Coalition mobilized and disseminated online surveys to generate key insights around its impact on women's experiences in online contexts, and these survey results suggested an increase in reporting of

technology-facilitated violence during the pandemic, with women and girls disproportionately impacted.[44] Furthermore, these studies' more experimental nature allows for broader conceptualizations of TF VAW, or the inclusion of new and more context-specific forms of TF VAW – meaning they may be better suited to capture this phenomenon's impact on more diverse groups of women and girls.

Box 3.
Promising practices: CSO-driven data collection helps capture intersectional impacts of complex crises

Global evidence indicates that the COVID-19 pandemic significantly increased rates of online violence, with women and girls disproportionately impacted.[45] An online survey by advocacy organizations Glitch UK and the End Violence Against Women Coalition found that 38 per cent of women respondents experienced online abuse in the months preceding COVID-19. Of these, 27 per cent reported increased online abuse during the pandemic. These statistics were even greater for Black and minoritized women: with 50 per cent reporting online abuse before the pandemic, and 38 per cent saying it increased during COVID-19.[46] Importantly,

this survey also featured a more inclusive definition of online abuse, giving survey respondents the option to select from 28 types of behaviours.[47]

These findings align with those of UN Women's Regional Office for the Arab States, which, also using an online survey, found that online harassment was the highest reported type of violence against women in the region.[48] Based on this finding, UN Women conducted a follow-up, more in-depth investigation around online violence in the region. This included another series of targeted online surveys (one sent to a random selection of women online, and a second survey targeted at CSOs, women's activists and service-providers). This was complemented by qualitative research and a mapping of existing laws,

to identify forms of TF VAW, different at-risk groups and barriers to reporting, with targeted recommendations for responsible parties developed based on the findings.[49]

While there is long-established evidence that VAW increases during crises, unlike many past climate-induced disasters or armed conflicts, the COVID-19 pandemic was uniquely characterized by increased time spent online, as well as an "uptick in extremist and 'anti-minority mobilisation' and a proliferation of conspiracy theories and misinformation online scapegoating certain individuals and communities."[50] CSO research also helped raise awareness around new forms of violence associated with increased Internet usage, such as Zoom-bombing.[51]

QUANTITATIVE ADMINISTRATIVE DATA

Administrative data from institutions dealing with reported cases of VAW (including police, justice, health or social services) can provide valuable and timely evidence that is otherwise difficult (and costly) to capture through other research methods. Administrative data can shed light on the number of women and girls accessing services; which women and girls are most likely to access or use services; and provide information to evaluate programmes and policies, among other actionable insights.[52] Crucially, administrative data are also an effective way to obtain key insights without relying on methods like interviewing, particularly when the latter pose unnecessary risks or burdens for survivors.[53] Yet, this scoping review identified limited efforts to leverage available administrative data from governments, technology companies or other service-providers, to strengthen knowledge around TF VAW.

Service data

Quality administrative data from government and civil society services can provide useful insights on different forms of gender-based violence, including how reporting trends change over time, quality of services and estimated costs of service-provision.[54] While this paper identified an overall lack of government-based administrative data on TF VAW, there are signs of some emerging promising practices. For example, the national police of Morocco reported for the first time in 2020 that at least 1 per cent of reported VAW cases had been "committed by the means of modern technology," and this increased to 2 per cent in 2021.[55] Meanwhile, in Canada the police force uses a 'flag' to identify when any ICTs, including computers, phones, the Internet and other digital tools, are used in reported VAW incidents. However, this database does not include forms of violence that do not meet the criminal threshold but might be considered acts of TF VAW (such as discrimination and bullying).[56] Additional research is needed to identify promising practices for state-based administrative data collection on TF VAW, including how to integrate TF VAW into existing service-provision and data-collection efforts.

Transparency reports from technology companies

Many of the world's largest technology companies have endorsed The Santa Clara Principles on Transparency and Accountability in Content Moderation, and actively collect and share analysed data on the percentage of reported and addressed incidents,[57] some of which include forms of TF VAW. Yet, while technology companies have made important strides towards transparency and accountability in recent years, the nature of these data-collection and sharing mechanisms remains limited, particularly for action and advocacy to eliminate VAW.[58] Notably, all transparency reports reviewed for this paper[59] lack information on perpetrators and targets' age, sex and other key socio-demographic factors – a significant missed opportunity for understanding how women, girls and other groups disproportionately experience TF VAW. Advocates and recent audits[60] have also highlighted the ways in which many technology companies fail to report on the geographic context or scope of reported incidents of technology-facilitated violence (with some promising exceptions, like YouTube).[61] There is also a lack of guidance from most companies on how researchers can use what limited data are available (or explanations on why sharing certain data might put victims of technology-facilitated violence at greater risk of harm[62]). Lastly, technology companies' data-collection, transparency and content-moderation practices, overall, lack standardization. While some flexibility is necessary, given each technologies' unique features and services, greater standardization in companies' reporting practices would help researchers, policymakers and advocates compare efforts to understand and moderate technology-facilitated violence, including TF VAW.

QUALITATIVE DATA

This scoping review identifies qualitative data generated through more traditional approaches, like key informant interviews and focus group discussions with survivors, service-providers, policymakers and other relevant stakeholders, as well as newer approaches that may be useful for studying TF VAW. Consultations with impacted individuals, when conducted carefully and upholding the principles of survivor-centred research, are important for understanding the diverse ways in which different

forms of TF VAW impact particular groups of women. This includes the severe impacts of TF VAW on migrant women,[63] women with disabilities[64] and journalists.[65]

Indeed, a significant advantage of qualitative research is that such methods may provide researchers with the opportunity to explain TF VAW in a way that is more likely to be understood by different research participants, and thus overcome the barrier of a lack of a shared and well-known definition. Messing et al.'s interviews with residents of a women's shelter, for example, help illustrate how technologies are interwoven throughout women's experiences of stalking and abuse, making the distinction between 'offline' and 'online' violence blurry and irrelevant – especially given women's need to continue using digital technologies for their livelihoods and, indeed, to escape situations of violence.[66] Qualitative research with service-providers is another useful approach that has long been used and recommended to generate knowledge around VAW,[67] as it allows researchers to understand the nature of different forms of violence without asking survivors to repeatedly share their stories, which can create significant harm. Such approaches are also helpful in dismantling conceptions of an 'online/offline binary'.

This paper also identified innovative qualitative research methods that are uniquely fit for studying TF VAW, like digital (or virtual) ethnographies.[68] Similar to traditional ethnographies, digital ethnography "involves locating and situating the 'field' (a website or group), and learning about its cultural practices, social relations, languages, rituals, taboos and formal and informal rules within its own social, environmental and cultural context."[69] Henry and Flynn's 2020 study of image-based sexual abuse used this methodology to examine 77 sites that host such material. Their in-depth analysis of the online spaces where violence occurs allowed researchers to gain a unique understanding of the motivations and practices of perpetrators of TF VAW (which authors note is "far more complex than the paradigmatic 'ex-lover' revenge narrative"). It also provided insight into the ways in which online environments exacerbate risks of violence (such as the anonymity afforded by online spaces, as well as their over-visualization),[70] which can inform the design of targeted TF VAW prevention and response programmes.

Qualitative research, is critical for identifying the root drivers of and entry points for addressing TF VAW, illuminating complexities, and closing data gaps around how different groups are particularly targeted and impacted by this phenomenon. Given the unique capacity for qualitative methods to generate these types of actionable insights, academics, advocates and CSOs often leverage qualitative data to drive advocacy agendas. Indeed, academics and practitioners were investigating and striving to measure TF VAW long before states began integrating relevant variables into national surveys or administrative data systems.[71] Furthermore, given the ongoing evolution of digital technologies, new forms and modes of TF VAW are expected to continuously emerge. As such, more exploratory research methods, like key informant interviews, focus group discussions and digital ethnographies, are essential for identifying and understanding new forms of technology-facilitated violence, and identifying ways of including them in more official or generalizable quantitative studies, including national surveys and administrative data. Lastly, these methods are important for awareness-raising among research participants: feminists have long noted how participatory research methods, or research that starts from the standpoint or lived experiences of marginalized individuals, can contribute to the construction of collective understandings of oppression, and in doing so, contribute to movements building towards gender equality and gender justice.[72]

MIXED METHODS

Mixed methods studies leverage various qualitative and/or quantitative methods to enable innovative and more targeted analyses. For example, quantitative methods (such as population-based surveys) can be used to generate VAW prevalence rates, while qualitative methods (such as key informant interviews) can be used to describe and contextualize women's experiences with technology-facilitated violence, thereby shedding light on why and how such violence occurs.[73] Or, this approach can be reversed: qualitative research methods can be leveraged to develop descriptions and eventually typologies of TF VAW, and these can in turn inform the development of quantitative research tools.[74] This may also include bringing together different data sources, such as data from a population-based

survey, administrative data and publicly available social media data (see Box 4). Any particular methodology or type of data has its limitations, for the study of TF VAW or any other social phenomena.

As such, innovative approaches that combine diverse lived and epistemological perspectives are essential for addressing data gaps and ensuring a more comprehensive, in-depth and action-driven understanding of TF VAW.

Box 4.
Promising practices: Quantitative and qualitative methods to produce more actionable insights on TF VAW

A project by Australia's ANROWS, entitled "Technology-facilitated abuse: Extent, nature and responses in the Australian community" featured three research phases: 1) an online survey to capture support-service-workers' perspectives on the nature and impacts of TF VAW (termed "technology-facilitated abuse", or TFA); 2) in-depth interviews with survivors and perpetrators to understand their lived experiences, forms of TF VAW and the nature of perpetration; and 3) an online survey to establish nationally representative prevalence rates for the victimization and perpetration of identified types of TF VAW.

Through this multi-phased, mixed-methods approach, ANROWS was able to: advance national policy and research priorities; bridge pressing data gaps on the extent and nature of TFA; and identify evidence-based and practice-informed recommendations for improving policy frameworks, legal responses and support services for addressing TF VAW. Indeed, while the final phase (a nationally disseminated online survey) helped bridge important data gaps on the scope of TF VAW, prevalence data alone are insufficient for developing targeted government responses for protecting women and girls' rights to live a life free from violence. Instead, the additional phases (research with service-providers, then with survivors and perpetrators of TF VAW) helped produce a more in-depth understanding of lived experiences, key service barriers, and potential entry points for addressing and ultimately preventing this form of violence and abuse. In doing so, the ANROWS initiative illustrates the need for both quantitative and qualitative data-collection methodologies that capture the perspectives of different key stakeholders, in order to produce the actionable insights needed to advance survivor-centred response efforts and, ultimately, the prevention and elimination of TF VAW.

Note: See ANDROW's "Technology-facilitated abuse: Extent, nature and responses in the Australian community" research project and related publications here.

Social media data

One mixed-methods approach that was particularly evident in the reviewed literature was the use of qualitative and quantitative methods to collect and analyse social media data, sometimes referred to as "Big Data".[75] Ensuring that ethical standards of anonymity and confidentiality are strictly met, these methods can be particularly useful for studying forms of TF VAW that occur via social networking sites, including online harassment and gendered hate speech. All of the reviewed studies analysing social media data specifically use data from Twitter, which is likely due to the greater public access to this data (in other words, publicly available tweets). Such studies often begin with desk reviews and qualitative research to identify what language is relevant to the study's focus. For example, if the study is interested in violence against migrant women in a particular cultural context, they explore what language and terms should be included to capture the appropriate data set. Based on these more qualitative insights, researchers use computational methods — i.e., artificial intelligence (AI) and machine-learning tools — to scrape and analyse identified (and generally large) sets of publicly available data. A final research phase often includes the more in-depth qualitative, textual analysis of the identified sampling of social media data, so as to provide a more contextual understanding of different forms of TF VAW.[76]

Given the speed at which hateful, threatening and abusive content is created and shared, AI-based methods for detecting technology-facilitated violence are important and necessary. The methods described here are useful for experimenting with different techniques for identifying and even preventing online violence, and thus informing the strategies used by technology companies and their content moderators. That said, computer and social scientists alike have long critiqued the use of AI as a primary means for moderating online content, given its significant limitations. For example, these tools have: biases towards the life experiences of those creating them (and women are underrepresented in STEM fields[77]); low accuracy (given the speed at which language associated with TF VAW may develop and change, nuances in online behaviour depending on cultural contexts,[78] or the relationship between victims and perpetrators); unclear and inconsistent definitions of TF VAW (or, 'community policy violations'); and lastly, there is a lack of transparency on how moderation tools are developed and used by technology companies.[79] Together, these and other limitations result in AI-based methods missing certain incidents of TF VAW, which, when also unreported by moderators and/or individual content users, may create significant risks to targets of abuse.

Box 5.
Promising practices: Combining survey, administrative and social media data to illustrate TF VAW

Research in the United States by Blake et al. illustrates the innovative potential of bridging diverse data sets to understand the relationship between online and offline VAW — and consequently, the need to invest in diverse data sources to strengthen knowledge generation around TF VAW. The authors used three types of data in their study: population-based survey data (American Community Survey), administrative data (crime data from the Federal Bureau of Investigation), and social media data to investigate the relationship between hate speech and incidents of domestic and family violence. In triangulating the data sets, a key finding surfaced for advocates and policymakers: misogynistic tweets are directly correlated with increased incidents of violence across 47 US states. Given that these data are nationally representative and come from generally trusted sources (the FBI and the US Census), they have the potential to significantly contribute to advocacy and awareness-raising efforts. Including forms of TF VAW in NSO and administrative data-collection systems, while ensuring that individual anonymity and confidentiality are prioritised, could help advance these types of important and needed — yet generally lacking — nationally representative studies.

Source: Blake, K.R., S.M. O'Dean, J. Lian, and T.F. Denson. 2021. "Misogynistic Tweets Correlate with Violence Against Women." Psychological Science 32 (3): 315–25.

Current state of evidence and data

This phased scoping review methodology identified: **34 empirical studies** that analyse original evidence on the forms, contexts, prevalence, drivers, risk factors and impacts of TF VAW; **10 evidence reviews** that synthesize relevant studies; and **nine commentaries or guidance** relevant to collecting data on TF VAW.

Notably, 80 per cent of the sources captured in the scoping review were published between January 2019 and July 2022, suggesting that research on TF VAW is still relatively nascent.[80] Despite language limitations, there was relatively diverse geographical representation among the empirical studies. Certain aspects of TF VAW are more studied than others: most reviewed articles focus on the forms and prevalence of TF VAW; some studied its impacts; while fewer articles studied risk factors and drivers as well as contexts of TF VAW.

FORMS OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

→ **What is studied:** States, advocates and scholars largely disagree on what 'counts' as TF VAW. The more inductive approach of many qualitative studies often resulted in a broader analysis of technology-facilitated sexual violence, harassment, bullying, coercion, stalking and exploitation. In contrast, quantitative studies often employed more limited conceptualizations of TF VAW. Relatedly, few studies compared how different technology-based tactics are used for perpetrating VAW. Of those that took this approach, most largely focused on unwanted messaging or posts (24 out of 34 articles); threats (20 articles); or image-based forms of abuse (20 articles). Other tactics are less commonly studied, including: doxing (seven articles); hacking (10 articles) and impersonation (11 articles).

→ **Key trends:** Among the few studies that compare different forms of TF VAW (including sexual harassment, stalking, bullying, hate speech, sexual exploitation, non-consensual pornography, and defamation, among others), most found that sexual harassment and stalking were the more commonly reported forms of technology-facilitated violence experienced by women.[81] However, it is important to note that the specific rates developed from these studies cannot be compared, given their unique methodologies and sampling approaches. Of the studies that compared technology-based tactics, several found that the most common technology-based tactics for perpetrating sexual harassment are image-based abuse[82] and unwanted messages, posts and phone calls.[83] While such findings may be used to justify the prioritization of these forms and tactics of abuse, this may illustrate the need for more foundational research with broader definitions of TF VAW.

CONTEXTS OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

→ **What is studied:** Social networking sites are the most commonly studied context of TF VAW (21 out of 34 articles), followed by communication technologies (15 articles) and personal online accounts (12 articles). More specifically, email, Twitter, Facebook, Instagram and WhatsApp were some of the most commonly mentioned contexts where VAW is perpetrated. Far fewer research studies investigate violence on dating or entertainment sites, as well as GPS-based and 'smart home' technologies.

Key trends: Of the studies that compared different contexts of TF VAW, many found that women were more likely to experience violence on social networking sites, compared to other digital contexts.[84] While several social media platforms were mentioned (including Twitter, WhatsApp, Instagram and Reddit), across diverse world regions, Facebook (by Meta) was consistently identified as the most common site for online gender-based violence.[85] As past evidence reviews have noted, these findings should be understood in context of the scale of Facebook's popularity compared to other social media platforms, and the distinct risks associated with open chat platforms, compared to private messaging services.[86]

RISK FACTORS OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

What is studied: Little evidence has been generated on potential risk factors or drivers of TF VAW. Of the studies reviewed, most are led by CSOs and academics, yet these often lack the sample size, diversity of study participants, and/or collection of variables needed to identify which groups are at greatest risk of which types of technology-facilitated violence or compare risk factors across contexts. At the same time, most population-based studies lack an intersectional analysis in the presentation of their findings. While data findings are often disaggregated by age and sex, few include variables like sexual orientation, gender identity, income, race, ethnicity, dis/ability or migrant status in their analysis. Different uses of statistical denominators also complicate comparable analyses of risk factors.

Key trends: Studies that include both men and women illustrate that: violence in digital contexts affects everyone[87] but women are more likely to experience more *severe* forms of technology-facilitated violence (such as sexual harassment and stalking) compared to men;[88] that women and non-binary individuals who report online violence are often targeted *because of* their sex and gender identity;[89] and that discriminatory gender norms are a commonly cited driver of TF VAW.[90] Of the

relatively limited set of studies that do include a more comprehensive collection of variables, thus allowing for more in-depth intersectional analysis of experiences with TF VAW, these largely find that subgroups of women that are at heightened risk of offline violence are also at greater risk of online violence, including: young women and girls;[91] women in public life;[92] lesbian, gay, bisexual, transgender, intersex, queer and other (LGBTIQ+) people;[93] racialized, minoritized and migrant groups of women;[94] and women with disabilities.[95] These groups' experiences with online violence are driven by structural inequalities and intersecting forms of discrimination, which are at times exacerbated by certain digital-specific risk factors.

IMPACTS OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

What is studied: Perhaps due to the need to convince policymakers and other key stakeholders that TF VAW 'matters', a large share of the reviewed articles (16 out of 34) had the primary objective of analysing the impact of different forms of TF VAW. These were largely led by academics and CSOs and used a range of qualitative and quantitative research methods to detect the gendered impacts of TF VAW.

Key trends:
- TF VAW, particularly among social networking platforms, **promotes cultures of violence, including the normalization of misogyny and VAW**.[96] Technology-facilitated violence "toxif[ies] public discourse and motiv[ates] other forms of extremist and hateful behavio[ur] through a cycle of 'cumulative extremism'."[97]

- **The impacts of TF VAW are often as severe as offline VAW.** New digital technologies may increase the risks and severity of offline VAW (e.g., GPS technologies can be used to target, track and inflict physical violence). Furthermore, the emotional impacts of online violence are especially well documented:[98] In 2014, UNICEF reported that the risk of suicide attempts was 2.3 times higher for victims of cyberharassment, compared to non-victims.[99]

- Along with the direct harm caused by TF VAW, online violence is also **connected to offline acts of physical, sexual and emotional violence as part of the continuum of violence.**[100] For example, evidence from the US found that victims of online sexual dating abuse were seven times more likely to have also experienced offline sexual violence.[101] Global research on violence against women journalists also illustrates how online violence may result in further acts of harm against survivors' networks (such as colleagues, family members or friends).[102]

- TF VAW **also contributes to the gender digital divide.** Reviewed studies found that TF VAW is changing the way women interact in both online and offline contexts, which has significant political and economic consequences.[103] One online survey on sexual harassment among Egyptian women during the COVID-19 pandemic found that 6.4 per cent of women left social media due to experiences of online violence.[104]

- Online platforms were once viewed as a force for democratization, providing new opportunities for previously marginalized groups to more equitably engage in politics and policymaking. Yet the rising threats of TF VAW **stifle women's voices and infringe on women's rights to political participation**.[105] Research has shown how women in politics and women journalists are particularly targeted, and how these experiences often drive them out of these professions.

- Likewise, engagement with digital technologies and tools is considered by many to be key for taking advantage of new economic opportunities. Yet, with women leaving online platforms due to experiences or concerns of TF VAW (i.e., the growing global gender digital divide), **women are increasingly excluded from such economic opportunities**.[106] For example, in face-to-face surveys in Malawi, 76.1 per cent of women said gender-based cyberviolence resulted in a loss of income, and 12 per cent reported losing new employment opportunities.[107]

Challenges

The following section outlines a three-fold categorization of overarching challenges stymying data collection on TF VAW. These challenges are key both for elucidating the current state of evidence on TF VAW and identifying strategic entry points for action to address knowledge and data gaps, including by adapting existing methods and approaches, or developing new ones. It is important to note that each of these challenges is deeply interconnected.

METHODOLOGICAL CHALLENGES

1. **Lack of a shared operational definition and methodology for monitoring, measuring and analysing** TF VAW**.** One of the clearest findings from this evidence review (as others[108]) is the lack of a consistent, standard and shared definition of TF VAW (as an umbrella term) among key stakeholders, as well as a lack of common vocabulary on its forms and modes (for example, how to categorize different tactics or manifestations of TF VAW, like image-based abuse and harassment, or how to understand the different 'spaces' where TF VAW occurs, like social networking sites or dating applications). At the same time, while narrow conceptualizations of TF VAW may seem more practical from a research perspective, or a desire for global comparisons, such conceptualizations run the significant risk of overlooking the many ways in which ICTs and other digital tools impact *all* women and girls. Broader conceptualizations (which also require leveraging more diverse data sources and methodologies) are needed to ensure TF VAW research and investments uphold SDG commitments to leave no one behind.

2. **Lack of shared indicators for intersectional analysis.** Relatedly, there isn't yet a shared understanding around what data points are most actionable and of greatest priority for generating knowledge on TF VAW (data on where the act of TF VAW took place, frequency of incidents, impacts of violence, relationship with perpetrators, and/or other factors?) There are also different approaches regarding what

'denominator' is most relevant for studying TF VAW (the prevalence of TF VAW among *all women*, or *women currently online*?) This results in inconsistent reporting systems or response policies across different digital platforms, technologies and tools. Moreover, most available data on TF VAW also lacks disaggregation by age, sex or other important socio-demographic factors, thus limiting possibilities for understanding technology-facilitated violence's disproportionate impacts on women, girls and gender minorities, as well as an intersectional analyses of the trends, drivers and impacts of TF VAW.[109]

3. **Limitations of social media data.** In many ways, AI-based research methods are needed for investigating TF VAW, given the speed and breadth of online interactions and primary and secondary acts (and impacts) of online violence. However, social media data, and AI-based tools for analysing this data, are inherently limited as they rely on *very* particular assumptions and data sets, so great care must be taken in interpreting their results. In addition, while progress has been made to advance machine-learning tools for identifying hate speech, these require continued investment and attention to ever-changing local dynamics (for example, new trends in VAW and misogynistic language, or new forms of online violence). Furthermore, while AI-based methods are useful for analysing large data sets, they are less suited to investigating context-specific drivers of VAW, which are essential to understand and identify entry points for change and to inform local prevention and response services. Lastly, the highly experimental nature of such methods makes comparison across studies difficult, or near impossible.[110]

ETHICAL CHALLENGES

1. **Privacy and protection.** While more transparency from technology companies on their practices for monitoring TF VAW would contribute to building greater understanding of its forms,

patterns and dynamics, significant caution must be taken to ensure data-sharing does not violate individuals' privacy or create additional risks of harm. This should be done for any data-collection exercise on TF VAW by any institution, adhering to ethical and safety guidance on the collection and use of VAW data (currently being updated by WHO). For example, if anonymized data from different technology companies were brought together for analysis, there is a possibility that one could identify individuals and expose intimate details of people's lives, including their geolocations. Likewise, while disaggregated data contribute to a more nuanced and intersectional understanding of TF VAW, there are necessary limits to disaggregation that need to be maintained to ensure that these data remain anonymized.[111]

2. **Survivor-centred training.** Specialized ICT surveys are important for addressing gaps in VAW-specific studies, particularly those by NSOs and other national partners, which often only include the perspectives of adult women. It is important that these specialized surveys also uphold international standards around survivor-centred research, as well as specific VAW standards research. This may be a challenge if data collectors are only trained in technology or digital development, rather than VAW prevention and response.

3. **Lack of response services.** Aligned with the broader literature on 'offline' VAW, some scholars question the ethics of collecting data from survivors of TF VAW without ensuring full privacy and access to necessary support services or protection mechanisms (such as effective restraining orders against cyberstalkers).[112] Again, this illustrates the cyclical nature of these interconnected challenges. Without sufficient data, state governments and service-providers may lack the information necessary to mobilize resources and craft appropriate and targeted support services and protection mechanisms. Yet, without support services and protection mechanisms, some scholars question the ethics of 'extracting' data from survivors.[113]

SOCIOPOLITICAL CHALLENGES

1. **Lack of overall problematization and awareness around** TF VAW. Based on the reviewed literature, TF VAW appears to be viewed as a new and niche issue, rather than a significant and pressing societal concern, despite evidence across diverse regional contexts illustrating the many ways in which it normalizes cultures of violence, fear and misogyny,[114] and increases risks of suicide,[115] sexual violence[116] and physical harm against women, girls and their communities.[117] This review suggests this is a cyclical problem: Due *in part* to a lack of data (and dissemination of data findings), there is a lack of awareness around the prevalence of, and harms caused by, TF VAW. Yet this lack of awareness or concern for TF VAW can in turn stymie prevention and response policies, programmes and services, which further impedes data-collection efforts. As is true more broadly of VAW, the lack of overall problematization and awareness around TF VAW can often also be traced to an absence of sufficient political will among those with decision-making power, who may cite insufficient evidence or 'proof' of a problem as a rationale for low investment or delayed action, both in data collection and service-provision.[118]

2. **Outdated legal frameworks, training and protection.** While noting some promising progress in a select number of countries, laws and regulations continue to lag significantly behind technological innovation. This includes a failure to include online violence in VAW-related laws, as well as a failure to recognize gendered violence in legislation or regulations pertaining to technology-facilitated violence and content moderation.[119] Often, laws are an important catalyst for changes to technology companies' policies, or for comprehensive updates to service-providers' training.[120] This poses a challenge for data-collection efforts, as service-providers' (including police, medical professionals, women's shelters, etc.) lack of training on technology-facilitated violence can lead to misidentification of acts of violence, and consequently, flawed administrative data sets, as well as flawed or inadequate responses (or a lack of response entirely).[121] Likewise, the exclusion of technology-facilitated forms of VAW from legal frameworks

may also contribute to (or be used to justify) their exclusion from NSO surveys, which thereby limits access to important population-based data.

3. **Need for significant (and timely) multi-stakeholder partnership and coordination.** No single actor alone can generate the data needed on TF VAW, given the unique role of global technology companies in 'governing' spaces where VAW takes place, the ubiquitous nature of ICTs, and the rapid and potentially cross-border impacts of TF VAW. The reviewed literature indicates the critical need for stronger partnerships and long-term coordination across international organizations, governments, technology companies, service-providers, data producers and researchers to develop appropriate reporting, monitoring and data-collection mechanisms.[122]

4. **The limited data that exist are often biased towards the Global North.** Like all forms of VAW, TF VAW (and the impacts of different forms on different subgroups) may vary across diverse contexts. For example, while a fully-clothed photo may not be considered sensitive in the Global North, in South Asia the non-consensual sharing of fully-clothed photos can cause significant emotional and psychological harm.[123] Yet, interventions and measurement tools developed and evaluated in high-income countries have often been parachuted into other settings without being properly adapted for these cultural nuances.[124] As some scholars have astutely noted, inequitable resource distribution contributes to this challenge: Evidence suggests that some technology companies spend fewer resources to contextualize their products for lower- and middle-income countries.[125]

Conclusion and key recommendations

The digital revolution holds the potential to advance women and girls' rights – from expanding access to educational and economic opportunities and enabling paths for political participation, to strengthening access to essential services and building transnational feminist communities. Yet, such benefits will be severely constrained for many as long as TF VAW remains unaddressed and underrecognized as a serious violation of women's rights. Indeed, this paper reveals that women change their online behaviour or stop using certain ICTs altogether due to TF VAW, exacerbating the global gender digital divide. TF VAW not only undercuts the potential benefits of the digital revolution, but it constitutes a direct violation of women's rights and stymies progress towards gender equality and women's empowerment. Furthermore, given the unique speed, reach and ubiquity of today's technologies, this form of violence also contributes to normalizing VAW and misogyny.

Quality and timely data on TF VAW are needed to inform the design of targeted, context-specific policies, programmes and services. Yet, while feminist scholars and women's rights activists have long been sounding the alarm bells about the new tactics and forms of gendered violence facilitated by ICTs and 'new' digital contexts, significant gaps remain – both in state action and data collection. This paper has identified gaps in global, regional and national prevalence data and administrative data. While technology companies have made important strides on transparency and accountability in recent years (largely in response to CSOs' advocacy and public pressure), this paper and others have identified gaps in their reporting on TF VAW. Furthermore, across all reviewed data sources, this paper found a lack of sex, gender identity - and age-disaggregated data, data on more diverse forms and modalities of TF VAW, and data from low- and middle-income countries. Investing in qualitative and quantitative research as well as triangulating diverse data sets is key for developing more intersectional and comprehensive analysis of the many forms of TF VAW, the differential impacts on *all* women and girls, and the drivers of and entry points to address it. In particular, while online surveys are useful, it is important to also invest in offline data-collection mechanisms, to capture experiences of technology-facilitated violence against women who lack access to or control over ICTs, or are not using the Internet for many other reasons (including, for example, past experiences or fear of

TF VAW). Together, these actions are essential for crafting appropriate responses, whether from Member States, UN agencies, technology companies and other responsible parties.

> **No 'data for data's sake', but data that is clearly tethered to and informs awareness-raising, advocacy and programmatic or policy design.**

Having more data, and more globally comparative data, is essential for catalysing action on TF VAW. However, this paper highlights the need for more than methodological guidance (although this is also paramount). As is the case with VAW more broadly, while data gaps are one reason for the relative lack of action on TF VAW, they hold insufficient explanatory power. Indeed, this paper makes clear that much *is* known about TF VAW; so, where responsible parties ignore the scope and gravity of TF VAW, and instead treat it as a minor or 'niche issue', this may signal a lack of political will. One strategy for ensuring that decision-makers cannot use the absence of data to explain their lack of response to TF VAW is to ensure that investments are made in research and data that is tied to action. In other words, not 'data for data's sake', but data that is clearly tethered to and informs awareness-raising, advocacy and programmatic or policy design. This requires increased investment in national surveys and administrative data collection, but also in qualitative and quantitative research by advocates, practitioners and academics. The latter is essential for generating the more in-depth studies needed to identify and address the drivers and impacts of TF VAW, as well as its many new and emerging forms, modalities, tactics and platforms. Furthermore, much greater efforts are needed on the part of technology companies to reduce barriers for sharing anonymized data with researchers, or to safely collaborate with states in data production and analysis efforts.

With this in mind, this paper concludes with targeted recommendations for UN agencies, Member States, technology companies and CSOs to address identified challenges and data gaps around TF VAW, so as to generate data that will be used to inform the policies, programmes and services needed to eliminate VAW, in all its forms.

RECOMMENDATIONS TO ADDRESS IDENTIFIED CHALLENGES AND DATA GAPS FOR ADVANCING KNOWLEDGE OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

on TF VAW from low- and middle-income countries, where there are notable data gaps. This may require knowledge-sharing on how to customize studies based on local contexts.

1. Develop standardized definitions, methodologies, indicators and principles for data collection

→ Socialize the proposed common definition of TF VAW and build consensus through regional consultations around its operationalization for data collection and measurement.

→ Develop standards for data collection, analysis and use on TF VAW using different methodologies and sources, including surveys and administrative records, and quantitative as well as qualitative methods. The standards should include clear definitions of each specific form of technology-facilitated violence (e.g., image-based abuse, hate speech, impersonation, etc), as well as diverse tactics. This should be regularly revisited and added to, as new forms of TF VAW emerge. Standards should address disaggregation by age and sex at a minimum and, ideally, by sexual orientation, gender identity, race, ethnicity, rural/urban and disability status, among other socio-demographic factors, including those most relevant to local contexts, to enable intersectional analysis. This level of (multiple and granular) disaggregation should only be considered in analysis and reporting if it can be ensured that individuals cannot be identified or have personal information exposed, as the privacy and safety of individuals should be paramount.

→ Standards should be built on the research and advocacy of civil society organizations (CSOs), feminist movements and other gender equality advocates, with broad global representation, to regularly revisit and refine the methodologies, to respond to the priorities and perspectives of survivors, and to identify new forms, tactics, and contexts of TF VAW as they emerge, as they are often more action-oriented and grounded in the priorities and perspectives of survivors.

→ Invite technology companies to participate in the development of these standards, as they may have unique insights around privacy rights and other technological considerations.

→ Ensure standards are relevant and applicable globally, so that they enable evidence-generation

2. Investments

→ Invest in qualitative research, which is key for identifying new and emerging forms of violence, and thus informing the development of quantitative survey instruments.

→ Invest in independent studies and citizen-generated data, particularly by CSOs, which are more nimble and thus capable of capturing diverse forms of TF VAW, as well as reaching diverse groups who may otherwise be underrepresented in such studies.

→ Provide training to governments, CSOs, data producers and researchers to address existing data gaps and inform context-specific and evidence-driven prevention and response programmes for TF VAW.

3. Legislation and norms

→ Member States should extend legal definitions of and policies regarding VAW to include TF VAW. Doing so contribute to setting a clear norm that these forms of violence are a violation of women's and girls' rights and will not be tolerated, and it will also help catalyse further action to build a shared understanding of what TF VAW is to inform data collection that is comparable across sectors.

→ Legislation should build on international standards and require technology companies, provided ethical safeguards are in place, to share a common set of metrics, including forms of TF VAW, disaggregated minimally by age, sex and gender identity, as well as on the geographic context of incidents of technology-facilitated violence, acknowledging that individuals and cases should not be identified for privacy and safety reasons.

→ Legislation should include as part of the TF VAW definition a comprehensive set of technologies or any digital tools that may assist, aggravate or amplify VAW, rather than only including online platforms or social networking sites.

4. Moving forward: Future research

→ While there is growing evidence of how digital technologies facilitate various forms of VAW including intimate partner violence, sexual harassment, stalking and hate speech, more research is needed on how they contribute to other forms of violence across the continuum, like human trafficking and other forms of exploitation, as well as religious and political extremism.

→ Evidence is also needed on more diverse tactics of online violence, including Zoom-bombing, trolling, doxing, impersonation, hacking and misinformation.

→ Lastly, much of the existing evidence analyses violence on social networking sites. Thus, more data is needed on other modes for ICT-facilitated violence, including GPS technologies, drones and other 'smart technologies', as well as dating, gaming and entertainment sites.

Annex A: Glossary of terms

Bullying: "An ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to cause physical, social and/or psychological harm. It can involve an individual or a group misusing their power, or perceived power, over one or more persons who feel unable to stop it from happening."[126]

Contexts of TF VAW**:** The different digital 'locations' where VAW may take place, such as social networking sites, personal online accounts, gaming and entertainment sites, or direct messaging platforms.

Defamation: "The act of communicating false statements about a person that injure the reputation of that person."[127]

Doxing: "The action of finding or publishing private information about someone on the Internet without their permission, especially in a way that reveals their name, address, etc."[128]

Exploitation: An act of abuse and coercion "where some form of remuneration is involved or whereby the perpetrators benefit in some manner — monetarily, socially, politically, etc."[129]

Forms of TF VAW**:** Different violent and abusive behaviours that fall under the broader umbrella term 'violence against women and girls', including: bullying, stalking, defamation, sexual harassment, exploitation and hate speech. Technology-based tactics can be used to perpetrate these forms of abuse, but they can also be perpetrated without the use of technology.

Hacking: "The activity of using a computer to access information stored on another computer system without permission, or to spread a computer virus."[130]

Hate speech: "Hate speech includes written, spoken or visual discrimination, harassment, threats or violence against a person or group on the basis of their gender, disability, sexual orientation, race, etc. Any speech that trivialises, glorifies or incites violence against women is hate speech, just as speech that trivialises the Holocaust is anti-semitic and speech that glorifies attacks on people because of their race is racist."[131]

Image-based abuse: "The sharing of (or threat to share) intimate images without the consent of the person in that image... Image-based abuse is often referred to as 'revenge porn' or 'cyberharassment.' Other terms used to explain this form of abuse include: sexploitation or sextortion, where someone blackmails another person by threatening to reveal explicit images; and e-venge, referring to the electronic distribution."[132]

Impersonation: "Creation of a hoax social media account, often using the target's name and/or photo, to post offensive or inflammatory statements to defame, discredit, or instigate further abuse. A harasser can also impersonate someone the target knows in order to cause harm."[133]

Prevalence of TF VAW**:** The share of a population that has experienced TF VAW, which is sometimes assessed over a specific time period ("have you experienced TF VAW within the last year?") or over one's lifetime ("have you ever experienced TF VAW?").

Risk factors and drivers of TF VAW**:** Variables that are associated with a greater vulnerability to or likelihood of experiencing TF VAW.

Sexual harassment: "An unwelcome sexual advance, unwelcome request for sexual favours or other unwelcome conduct of a sexual nature which makes a person feel offended, humiliated and/or intimidated, where a reasonable person would anticipate that reaction in the circumstances."[134]

Stalking: "A pattern of repeated and unwanted attention, harassment, contact, or any other course of conduct directed at a specific person that would cause a reasonable person to feel fear."[135]

Technology-based tactics of VAW: Specific strategies for perpetrating violence against women and girls that leverage technology, such as doxing, hacking, image-based abuse, and unwanted messaging or posting.

Threats: "A suggestion that something unpleasant or violent will happen, especially if a particular action or order is not followed."[136]

Annex B: Methodology

Search strategy

This paper used a phased scoping review methodology.[137] This entailed targeted searches of academic and grey (policy or programmatic) literature.[138] Key search terms were selected by referring to existing conceptual frameworks.[139] The primary questions driving this review focused on identifying what the available evidence said about: (1) The **forms, prevalence, risk factors,** and **impacts** of TF VAW, and what data are missing; (2) the challenges to collecting data on TF VAW; and (3) the potential **opportunities** for strengthening data collection on TF VAW. To supplement this targeted search, the researchers also drew upon the existing and burgeoning scholarship on gender, development and ICTs. Much of this literature examines the prevalence and dynamics of online and technology-facilitated violence, but because it is not often framed using the language of 'data', it was not always captured in the targeted scoping review. This paper also explored what women and young women feminist activists are saying and doing about this violence.[140]

Limitations

Adequately representing the state of data and data collection on TF VAW is an ambitious task, considering the variety of data types or sources and the lack of definitional consensus. Thus, this paper adopted a more inclusive working definition that captures both online violence and offline violence that is facilitated by ICTs, although doing so made including all relevant search terms a challenge. Furthermore, this study only includes articles published in English, with a few exceptions for state-produced data. Lastly, studies that investigate protective factors, help-seeking behaviours, characteristics of perpetrators or perceptions of TF VAW were excluded from this study, given its restricted scope. Future research is needed to identify trends in the literature around these subtopics.

With these limitations in mind, the present scoping review does not claim to capture all the available and relevant data. Rather, it is focused on describing key trends in a nascent field in order to inform recommendations for strengthening the understanding and measurement of TF VAW, including through subsequent systematic reviews of particular data sources, such as public administrative data sets.

Endnotes

1   O'Donnell, A., and C. Sweetman. 2018. "Introduction: Gender, development and ICTs." *Gender & Development* 26 (2), pp. 217–229.

2   Zulver, J., T.P. Cookson, and L. Fuentes. 2021. "COVID-19 and gender-based violence: reflections from a 'data for development' project on the Colombia–Venezuela border." *International Feminist Journal of Politics*; Handapangoda, W. and A. Kumara. 2017. "The World at Her Fingertips?: Examining the Empowerment Potential of Mobile Phones among Poor Housewives in Sri Lanka." *Gender, Technology and Development* 17 (3), pp. 361–385; Zelezny-Green, R. 2018. "'Now I want to use it to learn more': using mobile phones to further the educational rights of the girl child in Kenya." *Gender & Development* 26 (2), pp. 299–311.

3   Baker, S. 2018. "'We want that for ourselves': how girls and young women are using ICTs to counter violence and demand their rights." *Gender & Development* 26 (2), pp. 283–297; Titus, D. 2018. "Social media as a gateway for young feminists: lessons from the #IWillGoOut campaign in India." *Gender & Development* 26 (2), pp. 231–248; Muir-Bouchard, S. 2018. "Using digital technology to engage and mobilise young people to end violence in intimate relationships: lessons from Bolivia." *Gender & Development* 26 (2), pp. 341–358; Mecky, M. 2019. "Riding the Cyber Wave: How Feminist Activism Develops Strategies Against Gender-Based Violence." European Institute of the Mediterranean website. For example, Mecky 2019 points out that online activism is especially important for feminist movements and organizations who are particularly resource constrained. Beyond leveraging 'online spaces', in recent years civil society initiatives that leverage digital technologies to prevent and respond to gender-based violence have sprung up around the world. See for example HarassMap (Egypt), Cosas de Mujeres (Colombia); and Safetipin (started in India, now in multiple countries and regions). Meanwhile, Take Back the Tech is a collaborative global campaign that encourages women and girls to leverage their own ICTs to shed light on and challenge technology-facilitated violence against women.

4   Hussain, F., and S. Amin. 2018. "'I don't care about their reactions': agency and ICTs in women's empowerment in Afghanistan." *Gender & Development* (26) 2, pp. 249–265.

5   O'Donnell and Sweetman 2018.

6   Spuy, A. and N. Aavriti. 2018. "Mapping Research in Gender & Digital Technology." Ottawa: IDRC, p. 38.

7   O'Donnell and Sweetman 2018; Harris, B. and L. Vitis. 2020. "Digital intrusions: Technology, spatiality and violence against women." *Journal of Gender-Based Violence* 4 (3), pp. 325–341.

8   UN Women 2022a. "Accelerating efforts to tackle online and technology-facilitated violence against women and girls." New York: UN Women. p. 7.; Spuy and Aavriti 2018, p. 38.

9   Harris and Vitis 2020.

10 Posetti, J., N. Aboulez, K. Bontcheva, J. Harrison, and S. Waisbord. 2020. "Online violence against women journalists: a global snapshot of incidence and impacts." Paris: UNESCO; UN Women 2022b. "Violence Against Women in The Online Space: Insights From Multi-Country Research In The Arab States." New York: UN Women; UN Women. 2020b. "Rapid Assessment: The Effects of Covid-19 on Violence Against Women and Gendered Social Norms." New York: UN Women; Glitch UK and the End Violence Against Women Coalition (EVAW Coalition). 2020. "The Ripple: COVID-19 and the Epidemic of Online Abuse."

11 UN Women. 2023. "Technology-facilitated violence against women: Report of the foundational meeting of the expert group."

12 HRC (Human Rights Council). 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." A/HRC/38/47. p. 7.

13 Hinson, L., L. O'Brien-Milne, J. Mueller, V. Bansal, N. Wandera, and S. Bankar. 2019. "Defining and Measuring Technology Facilitated Gender-Based Violence." Washington, DC: International Centre for Research on Women (ICRW).

14 HRC 2018, p. 5. See also UN Women 2022a.

15 Medeiros de Araújo, A., C. Vieira do Bonfim, M. Bushatsky, and B. Alencar Furtado. 2022. "Technology-Facilitated Sexual Violence: A Review of Virtual Violence against Women." *Research, Society and Development* 11 (2), p. e57811225757; Cotter, A., and L. Savage. 2019. "Gender-Based Violence and Unwanted Sexual Behaviour in Canada 2018: Initial Findings from the Survey of Safety in Public and Private Spaces." Ottawa: Statistics Canada; Buchanan, N., and A. Mahoney. 2021. "Development of a Scale Measuring Online Sexual Harassment: Examining Gender Differences and the Emotional Impact of Sexual Harassment Victimization Online." *Legal and Criminological Psychology* 27 (1), pp. 63–81.

16 Buchanan et al. 2021; Pew Research Center. 2021. *The State of Online Harassment.*

17 Posetti et al. 2020; Iyer, N., B. Nyamwire, and S. Nabulega. 2020. "Alternate Realities, Alternate Internets: Feminist Research for a Feminist Internet." *Pollicy*, citing Zweig et al. 2013.

18 World Bank. 2022. "Online Violence Against Young Female Workers: Risks, Threats and Mitigation Strategies." Solutions for Youth Employment (S4YE) Knowledge Brief series: Issue 19; Malanga, D. 2021. "Survey of Cyber Violence against Women in Malawi." *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development, 2021*, pp. 623–34; Posetti et al. 2020; Economist Intelligence Unit. 2021. "Measuring the Prevalence of Online Violence against Women."

19 Noting the scope of these and other harms being enacted through online and ICT-facilitated violence, a recent report by the Special Rapporteur on violence against women and girls, its causes and consequences, emphasizes that women's rights to live a life free from violence, to freedom of expression, to privacy, to have access to information shared through ICTs, should also be protected in digital contexts, "including through the prohibition of gender-based violence in its ICT-facilitated and online forms." United Nations Special Rapporteur on violence against women, its causes and consequences. 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 (A/HRC/38/47), pp. 5–6.

20 UNESCO and UN Women. 2019. *The big conversation: Handbook to address violence against women in and through the media*; O'Donnell and Sweetman 2018; Spuy and Aavriti 2018, p. 78.

21 UN Women and WHO (World Health Organization). 2020. "Violence Against Women And Girls Data Collection during COVID-19."

22 HRC. 2021. "Gender justice and freedom of expression - Report of Special Rapporteur on the promotion and protection of freedom of opinion and expression." A/76/258.

23 Fuentes, L. and T.P. Cookson. 2020. "Counting gender (in)equality? A feminist geographical critique of the 'gender data revolution'." *Gender, Place & Culture* 27 (6), pp. 881–902.

24 See Arksey, H. and L. O'Malley. 2005. "Scoping studies: towards a methodological framework." *International Journal of Social Research Methodology* 8 (1), pp. 19–32. As noted in the methodology (Annex B), in addition to the literature captured in the scoping review, this paper also draws upon the existing and burgeoning scholarship on gender, development and ICTs and advocacy materials from feminist organizations focused on online and technology-facilitated violence.

25 See Annex B for additional details on the methodology employed for this study.

26 Some countries with high levels of connectivity are now using online surveys to research the national prevalence of VAW. For example, see the 2021 *Survey on Gender-based Violence in Finland*. However, these surveys generally also provide the option of a paper-based survey, if preferred by respondents.

27 For example, see WHO. 2001. "Putting women first: Ethical and safety recommendations for research on domestic violence against women."

28 See the European Institute for Gender Equality's definitions relevant to VAW data collection here.

29 See UN Women, UNFPA and WHO's Decision Tree on VAW data collection.

30 WHO. 2021. "Violence against women prevalence estimates, 2018. Global, regional and national prevalence estimates for intimate partner violence against women and global and regional prevalence estimates for non-partner sexual violence against women."

31 In 2017, the WHO's Multi-Country Study was revised to include two questions on TF VAW (one question regarding the use of mobile technologies to monitor and control, and another question concerning sexually explicit messages or pictures).

32 INEGI (Instituto Nacional de Estadística y Geografía). 2022. "Encuesta Nacional sobre la Dinámica de las Relaciones en los Hogares: Principales Resultados."

33 Learn more about the survey and its design here.

34 This comment comes directly from discussion at UN Women's Expert Group Meeting in November 2022, and comments from representatives of Mexico's National Institute on Statistics and Geography.

35 Economist Intelligence Unit 2021; Flynn, A., A. Powell, and S. Hindes. 2021. "Technology-facilitated abuse: A survey of support services stakeholders." ANROWS Research Report: Issue 2; Flynn, A., S. Hindes, and A. Powell. 2022. "Technology-facilitated abuse: Interviews with victims and survivors and perpetrators." ANROWS Research Report: Issue 11; Powell, A., A. Flynn, and S. Hindes. 2022. "Technology-facilitated abuse: National survey of Australian adults' experiences." ANROWS Research Report: Issue 12; UN Women 2022a; Pew Research Center 2021.

36 Ibid.

37 For example, see UN Women. 2020a. "Online Violence Against Women in Asia: A Multicountry Study"; Iyer et al. 2020; Posetti et al. 2020.

38 FRA (European Union Agency for Fundamental Rights). 2020a. "A long way to go for LGBTI equality: Questionnaire."

39 FRA. 2020b. "Second European Union Minorities and Discrimination Survey" Questionnaire."

40 Including Glitch UK & EVAW Coalition 2021; Ouerghi, A.D. 2020. *Study on cyber-violence against LGBTIQ++ Individuals*; Iyer et al. 2020; MRA (Mobilising for Rights Associates). 2019. "Virtual Violence, Real Harm: Promoting State Responsibility for Technology-facilitated Gender-based Violence against Women in Morocco Action Research Report."

41 UN Women 2020b.

42   For example, Malanga 2021.

43   For example, see Glitch UK & EVAW Coalition 2021; Ouerghi et al. 2020; Iyer et al. 2020.

44   Posetti et al. 2020; UN Women 2020b; Glitch UK & EVAW Coalition 2021.

45   Ibid.

46   Glitch UK & EVAW Coalition 2021.

47   Ibid.

48   UN Women 2020b.

49   UN Women. 2022b.

50   Glitch UK & EVAW Coalition 2021.

51   Economist Intelligence Unit 2021.

52   Ibid.

53   See for example UN Women, UNFPA and WHO's Decision Tree on VAW data collection.

54   European Institute for Gender Equality. 2019. "Police and justice sector data on intimate partner violence against women in the European Union."

55   Royaume du Maroc. 2021. « Fiche: Lutte contre la violence et la discrimination à l'égard des Femmes. Contribution au Rapport de la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences soumis à la 47eme session du Conseil des Droits de l'Homme. »

56   Learn more about Canada's Uniform Crime Reporting Survey here.

57   For social networking sites, this generally refers to shared content; for digital tools like Uber, this refers to incidents between drivers and riders.

58   Singh, S. and L. Doty. 2021. "The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules." *New America*.

59   See technologycoalition.org; Meta's reports here; Twitter's reports here; YouTube's here; and Uber's reports here.

60   As noted in a recent UNESCO report on violence against women journalists: "Some interviewees described these US-based companies' incapacity to deal with diverse cultures and linguistic variations as particularly problematic. South African journalist and editor Ferial Haffajee said: 'They treat their users in Africa like a colonial outpost'." (Posetti et al. 2020, p. 5)

61   Posetti et al. 2020; Bradford et al. 2019.

62   Cookson, T.P., J. Zulver, L. Fuentes, and M. Langworthy. 2020a. "Building alliances for gender equality: How the tech community can strengthen the gender data ecosystem." Ladysmith.

63   Henry, N., S. Vasil, A. Flynn, K. Kellard, and C. Morteux. 2021. "Technology-Facilitated Domestic Violence Against Immigrant and Refugee Women: A Qualitative Study." *Journal of Interpersonal Violence*.

64   Harris, B. and Woodlock, D. 2021. "'For my safety' Experiences of technology-facilitated abuse among women with intellectual disability or cognitive disability." eSafety.

65   Dhrodia, A. 2018. "Toxic Twitter." Amnesty International.

66   Messing, J., M. Bagwell-Gray, M.L. Brown, A. Kappas, and A. Durfee. 2020. "Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement." Journal of Family Violence 35 (7), pp. 693–704.

67   See UN Women, UNFPA and WHO's Decision Tree on VAW data collection.

68   For example, see Henry, N. and A. Flynn. 2019. "Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support." *Violence Against Women* 25 (16), pp. 1–24; Hall, M., and J. Hearn. 2018. *Revenge pornography: Gender, sexuality and motivations.* Abingdon: Routledge; and Uhl, C.A., K.A. Rhyner, C.A. Terrance, and N. Lugo. 2018. "An examination of nonconsensual pornography websites." *Feminism & Psychology* 28, pp. 50–68.

69   Henry and Flynn 2019, p. 7.

70   Ibid.

71   See for example #*JournalistsToo* by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Amnesty International's *Toxic Twitter*, and the Frida Fund's *Safe Sexting*.

72   See for example Smith, D. 1992. "Sociology from Women's Experience: A Reaffirmation." *Sociological Theory* 10 (1), pp. 88–98; or Collins, P.H. 1990. *Black Feminist Thought: Knowledge, Consciousness and the Politics of Empowerment.* Boston, London: Unwin Hyman.

73   For example, see Messing et al. 2020; UN Women 2022b; MRA 2019; UN Women 2020a, among others.

74   Hinson, Laura, J. Mueller, L. O'Brien-Milne, and N. Wandera. 2018. "Technology Facilitated Gender-Based Violence: What Is It, and How Do We Measure It?" Washington, DC: International Centre for Research on Women (ICRW).

75   Rego, R. 2018. "Changing Forms and Platforms of Misogyny: Sexual Harassment of Women Journalists on Twitter." *Media Watch* 9 (3), pp. 472–485; Gallego Durán, M., E. Gualda, and C. Rebollo Díaz. 2017. "Women and Refugees in Twitter: Rethorics of Abuse, Vulnerability and Violence from a Gender Perspective." *Journal of Mediterranean Knowledge* 2 (1), pp. 37–58; Kumar, P., A. Gruzd, and P. Mai. 2021. "Mapping out Violence Against Women of Influence on Twitter Using the Cyber–Lifestyle Routine Activity Theory." *American Behavioral Scientist* 65 (5), pp. 689–711; Mondal, M., S. Araújo, S. Leandro and F. Benevenuto. 2017. "A Measurement Study of Hate Speech in Social Media." *HT 2017 - Proceedings of the 28th ACM Conference on Hypertext and Social Media*, pp. 85–94; Babvey, P., F. Capela, C. Cappa, C. Lipizzi, M. Petrowski, and J. Ramirez-

Marqueza. 2021. "Using Social Media Data for Assessing Children's Exposure to Violence during the COVID-19 Pandemic." *Child Abuse and Neglect* 116 (2).

76   For a more comprehensive description of mixed-methods approaches for computational and qualitative analysis of social media data, see Andreotta, M., R. Nugroho, M.J. Hurlstone, F. Boschetti, S. Farrell, I. Walker, and C. Paris. 2019. "Analyzing social media data: A mixed-methods framework combining computational and qualitative text analysis." *Behavior Research Methods* 51, pp. 1766–1781.

77   UN Women. 2020c. "The Digital Revolution: Implications for Gender Equality and Women's Rights 25 Years after Beijing."

78   See takeaways from World Wide Web Foundation's consultations with feminist activists on the subject, here.

79   For more on the limitations of automated social media content moderation, see Spandana Singh. 2019. "Everything in Moderation," *New America*. 22 July.

80   Though, notably, as far back as 2000, feminists and women's rights activists were cautioning against popular notions of ICTs as only or mostly "emancipatory" tools and were sounding the alarm bells about "the internet as a terrain of violence of many kinds." (Spuy and Aavriti 2018, p. 38).

81   Malanga 2021; Economist Intelligence Unit 2021; UN Women 2020a.

82   Hassan, F.M., F.M. Khalifa, E.M. El Desouky, M.R. Salem, and M.M. Ali. 2020. "Cyber Violence Pattern and Related Factors: Online Survey of Females in Egypt." *Egyptian Journal of Forensic Sciences* 10 (1); UN Women 2022b; Glitch UK & EVAW Coalition 2020.

83   INSTAT (Albanian Institute of National Statistics). 2018. *National Population Survey. Violence Against Women and Girls in Albania*; Cotter, A., and L. Savage. 2019. "Gender-Based Violence and Unwanted Sexual Behaviour in Canada 2018: Initial Findings from the Survey of Safety in Public and Private Spaces." Ottawa: Statistics Canada.

84   Hassan et al. 2020; Iyer et al. 2020; UN Women 2022a; Glitch UK & EVAW Coalition 2020; Uganda Bureau of Statistics (UBOS). 2021. "Uganda Violence Against Women and Girls Survey 2020."

85   Iyer et al. 2020; Posetti et al. 2020; UN Women 2022b.

86   Hicks, Jacqueline. 2021. "Global evidence on the prevalence and impact of online gender-based violence (OGBV)," Knowledge, Evidence and Learning for Development (K4D).

87   Powell, A., Scott, A. J., & Henry, N. (2020). Digital harassment and abuse: Experiences of sexuality and gender minority adults. European Journal of Criminology, 17(2), 199–223;

88   Pew Research Center 2021.

89   Ouerghi et al. 2020; Mondal et al. 2017; Pew Research Center 2021; Iyer et al. 2020.

90   Iyer et al. 2020; UN Women 2020a; UN Women 2020b; Glitch UK & EVAW Coalition 2021.

91   Sambasivan, N., A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Never, E. Bursztein, E. Churchill, S. Consolvo. 2019. "'They Don't Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia." *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1–14; Pew Research Center 2021; Economist Intelligence Unit 2021; Babvey et al. 2021; UN Women 2020b; UBOS 2021; FRA (European Agency for Fundamental Rights) 2014. *Violence Against Women EU-wide survey: Results at a glance*. Luxembourg: Publications Office of the European Union; Cotter and Savage 2019.

92   Kumar et al. 2021; Zagloul, N., M. Rasha, R.M. Farghaly, H. ELKhatib, S.Y. Issa, and S.M. El-Zoghby. 2022. "Technology Facilitated Sexual Violence: A Comparative Study between Working and Non-Working Females in Egypt before and during the COVID-19 Pandemic." *Egyptian Journal of Forensic Sciences* 12 (1); UN Women 2020a; UN Women 2022b; Posetti et al. 2020; Rego 2018.

93   Powell et al. 2018; Ouerghi et al. 2020; Sambasivan et al. 2019; Cotter and Savage 2019; Pew Research Center 2021.

94   Vidgen, B., H. Margetts, and A. Harris. 2019. "How Much Online Abuse Is There? A Systematic Review of Evidence for the UK." London: The Alan Turing Institute; Iyer et al. 2020; Gallego et al. 2017; Glitch UK & EVAW Coalition 2021; Pew Research Center 2021.

95   Ibid.

96   Powell et al. 2018; Vidgen et al. 2019; Iyer et al. 2020.

97   Vidgen et al. 2019, citing Eatwell 2006.

98   Powell et al. 2018; Sambasivan et al. 2019; Crooks, H.R. 2017. "An Intersectional Feminist Review of the Literature on Gendered Cyberbullying: Digital Girls." *Jeunesse: Young People, Texts, Cultures* 8 (2), pp. 62–88; Medeiros de Araújo et al. 2022; Messing et al. 2020; Iyer et al. 2020; Patel, U., and R. Roesch. 2022. "The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Systematic Review." *Trauma, Violence, and Abuse* 23 (2), pp. 428–43.

99   Iyer et al. 2020, citing UNICEF France 2014.

100 Sambasivan et al. 2019; Reed, L. A., L.M. Ward, R.M. Tolman, J.R. Lippman, and R.C. Seabrook. 2018. "The Association Between Stereotypical Gender and Dating Beliefs and Digital Dating Abuse Perpetration in Adolescent Dating Relationships." *Journal of Interpersonal Violence* 00 (0), pp. 1–25; Blake, K.R., S.M. O'Dean, J. Lian, and T.F. Denson. 2021. "Misogynistic Tweets Correlate with Violence Against Women." *Psychological Science* 32 (3), pp. 315–25.

101 Iyer et al. 2020, citing Zweig et al. 2013.

102 Posetti et al. 2020.

103 Sambasivan et al. 2019.

104 Zagloul et al. 2022.

105 Kumar et al. 2021; HRC 2018 ; Faith, B., and E. Fraser. 2018. "VAWG Helpdesk Research Report What Works to Prevent Cyber Violence against Women and Girls?" 212, pp. 1–16.

106 World Bank 2022.

107 Malanga 2021.

108 See for example USAID. 2020. "Select Gender-Based Violence Literature Reviews: the Impact of Information Communication Technologies on Gender-Based Violence." Washington, DC: USAID; Hinson et al. 2018; Hinson et al. 2019.

109 Crooks 2016; Easpaig, Brona N. G. and David Fryer. 2011. "Dismantling dominant sexual violence research without using the master's tools," *Gay & Lesbian Issues and Psychology Review*; Fileborn, Bianca. 2012. "Sexual violence and gay, lesbian, bisexual, trans, intersex, and queer communities," Australian Centre for the Study of Sexual Assault.

110 Fortuna, P., J. Soler-Company, and L. Wanner. 2020. "Toxic, Hateful, Offensive or Abusive? What Are We Really Classifying? An Empirical Analysis of Hate Speech Datasets." *LREC 2020 - 12th International Conference on Language Resources and Evaluation, Conference Proceedings*, pp. 6786–94.

111 Cookson et al. 2020a.

112 Messing et al. 2020.

113 Zulver et al. 2021.

114 Blake et al. 2021.

115 Powell et al. 2018; Sambasivan et al. 2019; Crooks 2016; Medeiros de Araújo et al. 2022.

116 Sambasivan et al. 2019; Reed et al. 2018.

117 Sambasivan et al. 2019; Reed et al. 2018; Posetti et al. 2020.

118 Fuentes and Cookson 2020; Zulver et al. 2021.

119 Elmi, N. 2021. Written evidence submitted by Bumble to UK Parliament. United Kingdom Parliament.

120 Singh and Doty 2021.

121 For example, most stalking laws in the United States depend on reporting to police a belief that reported stalking incidents will cause *physical harm*. Therefore, if the victim doesn't connect TF VAW with threats of physical harm, they may fail to receive any protection or have the incident 'logged' as violence in administrative data collection systems (Messing et al. 2020).

122 Cookson, T.P., R. Carlitz, L. Fuentes, and A. Berryhill. 2020b. "Survey on Gender Equality at Home Report: A gender data snapshot of life during COVID-19." Facebook/Data for Good.

123 Sambasivan et al. 2019.

124 Kumar et al. 2021; Sambasivan et al. 2019; Iyer et al. 2020; Redondo, I., J. Jaureguizar, M. Dosil, and N. Galende. 2022. "Measuring Cyber Dating Violence: Reliability and Validity of the Escala de CiberViolencia

en Parejas Adolescentes (Cib-VPA)" [original in Spanish]. Clínica y Salud, 33 (3), pp. 93–99.

125 Iyer et al. 2020; Sambasivan et al. 2019.

126 See the National Centre against Bullying definition of bullying at: https://www.ncab.org.au/bullying-advice/bullying-for-parents/definition-of-bullying/

127 See the Merriam-Webster definition of defamation, at: https://www.merriam-webster.com/dictionary/defamation

128 See the Cambridge Dictionary definition of doxing: https://dictionary.cambridge.org/us/dictionary/english/doxing

129 See the *The Routledge International Handbook of Young Children's Rights* definition of exploitation.

130 See the Cambridge Dictionary definition of hacking: https://dictionary.cambridge.org/dictionary/english/hacking

131 See the Take back the tech definition of gender-based violence: https://takebackthetech.net/know-more

132 See the Tech Safety definition of image-based abuse: https://techsafety.org.au/resources/resources-women/image-based-abuse/

133 See Pen America's definition of online impersonation: https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/#:~:text=time%20as%20well.-,Online%20Impersonation,in%20order%20to%20cause%20harm.

134 See the Australian Human Rights Commission's legal definition of sexual harassment in the workplace: https://humanrights.gov.au/our-work/sexual-harassment-workplace-legal-definition-sexual-harassment

135 Bellevue College. 2020. "Gender-Based Violence Prevention: Stalking." 23 November.

136 See the Cambridge Dictionary definition of a threat: https://dictionary.cambridge.org/us/dictionary/english/threat

137 See Arksey & O'Malley 2005.

138 Search terms that were used for the scoping review were, by category: Online VAWG: GBV; VAWG; VAW; IPV; harassment; abuse; violence; cyberviolence; cyberbullying; cybercrime; cyberstalking; discrimination; trafficking; exploitation; Zoom-bombing; trolling; gendertrolling; doxing; hacking; threats; image-based abuse; fake accounts; impersonation; gendered misinformation. Key digital platforms, tools and technologies: ICT-facilitated; technology-facilitated; ICT; digital; virtual; email; Reddit; Slack; Zoom; apps; gaming; games; entertainment; Twitter; Telegram; TikTok; YouTube; Tumblr; Instagram; Facebook; Metaverse; WhatsApp; Snapchat; Messenger; Weibu; Line. Data collection: Review; data; evidence; collection; measurement; measuring; monitor; collect; analyse; evaluate; national statistics; administrative data; service data.

139 The conceptual framework developed by the International Center for Research on Women (Hinson et al. 2018 and 2019) was used as a basis and extended to allow a broader research scope. Specifically, ICRW's distinction between forms, modes, and cross-cutting tactics of technology-facilitated violence was used in order to identify trends in how TF VAW is (and is not) measured.

140 As a starting point, see for example this Special Edition in the journal of *Gender & Development*.