IN BRIEF

GUIDANCE FOR POLICE ON ADDRESSING TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

1. Overview

Technology-facilitated violence against women and girls (TF VAWG) is a global problem that requires a comprehensive, multisectoral response. In recent years, feminist mobilization and advocacy have given rise to the adoption of international and regional frameworks that intensify calls for legislation to regulate TF VAWG. Many governments have introduced national laws[1] that require police to address and reduce TF VAWG and its harms. The police are often the first line of defense against perpetrators. Their actions can protect and improve the safety of victims/survivors of online abuse.

TF VAWG disproportionately affects women and girls. Online prevalence ranges from 16 to 58 per cent.[2] Women and girls who face intersecting forms of discrimination, including those related to their age, disability or ethnicity, as well as those in public and political life, are most affected.[3] TF VAWG occurs within an online–offline continuum of violence against women and girls (VAWG). Growing evidence suggests that it results in offline harms, including femicide.[4]

Technology affects how police respond to cases of VAWG. They may have to respond to incidents where a woman is stalked online and the stalker then appears at her workplace, or where a partner is abusing a woman at home and also monitoring and controlling her movements using GPS-enabled technology. Given the increasing availability of digital tools and spaces, police may also encounter new forms of VAWG facilitated through technology. These encompass non-consensual intimate image-sharing, including deepfakes produced using generative artificial intelligence,[5] zoom-bombing,[6] doxing[7] and gendered disinformation.[8] Some of these images or posts can serve as online catalysts, for example, for honor-based crimes in communities where family and community honor codes remain prevalent.[9] This offline translation of online harms disproportionately affects women and girls in certain cultural contexts, where perceived violations of honor norms through digital platforms can result in physical violence, forced isolation, or femicide.[10] TF VAWG perpetrators may be someone known to the victim, such as an intimate partner, or a stranger.

A definition of TF VAWG

Technology-facilitated violence against women and girls (TF VAWG) refers to any act that is committed, assisted, aggravated or amplified by the use of information communication technologies 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.

Source: UN Women. 2023. Expert Group Meeting Report: Technology-facilitated violence against women: Towards a common definition.

Purpose of this brief

This brief presents the main elements of the forthcoming *Guide for Police on Addressing Technology-Facilitated Violence Against Women and Girls.* It should be read in conjunction with the Handbook on Gender-Responsive Police Services for Women and Girls Subject to Violence.

It responds to the critical need for targeted and effective interventions to address TF VAWG, especially by law enforcement, that are gender-responsive, survivor-centred and trauma-informed.

The brief highlights some challenges and gaps that police face in responding to TF VAWG. It provides guiding principles[11] for the initial response and investigation to uphold the rights of victims/survivors, including where they want abusive content to be taken down rather than pursuing a criminal justice pathway. It emphasizes keeping perpetrators accountable. Examples of promising practices used by police in TF VAWG cases are followed by a checklist of "dos and don'ts" for effective police investigations.

2. Gaps and challenges in reporting and investigating TF VAWG cases

The evolving nature of TF VAWG creates challenges for police interventions. These include: a lack of legal frameworks that classify different forms of TF VAWG as crimes that police can investigate,[12] the limited capacity of police to recognize the severity of TF VAWG and the harm it causes victims/survivors,[13] the unwillingness of some digital platforms to take down abusive content[14] and/or share information[15] that would help to identify perpetrators who are anonymous or unknown to the victim/survivor, and the transnational nature of TF VAWG.[16] The rapid growth of artificial intelligence is now facilitating the spread of targeted disinformation and the proliferation of image-based abuse,[17] posing new challenges for law enforcement in investigating these crimes.

For victims/survivors, their initial contact with law enforcement impacts how they will navigate the justice system. A positive experience rests on the ability of police to demonstrate that they will take complaints seriously, are committed to protecting the victim's/survivor's immediate health and safety and will support them on their journey through the justice system.

The following section provides an overview of the main challenges and gaps for police when initially responding to and investigating cases of TF VAWG. Identifying these in each national context can help to develop protocols and standard operating procedures for effective responses.

Limited understanding by law enforcement of what TF VAWG is

There is a disproportionate burden on victims/survivors to identify and report TF VAWG to service providers, including the police.[18] Victims of crimes online are less likely than those of traditional crimes to report cases to police or other authorities.[19] This is due in part to limited police understanding of the specific harms of digital violence and the false assumption that these are less severe than other forms of violence, e.g., physical violence.[20] Victims may also not trust the police and criminal justice system and believe that their complaint will not be taken seriously. They may perceive police as lacking digital knowledge and competence to investigate TF VAWG.[21]

In addition, if TF VAWG is not clearly defined in criminal law, there may be confusion about which police unit is best placed to respond to complaints (such as cybercrimes units or specialized VAWG units).[22] This may result in limited coordination, delays and revictimization, even as harmful content continues to spread online, causing psychological harm to victims, a diminished sense of security and a distrust of online platforms. Such delays will inevitably affect the victim's confidence in the police, which may negatively influence the decision to participate in the police investigation.

Legislative limitations

There are significant gaps in national legislation addressing TF VAWG. Currently, almost half of women globally lack legal protection against TF VAWG.[23] In some cases, addressing this violence may be perceived as competing with other fundamental rights, such as to privacy and freedom of speech, and the rights of the accused.[24]

As outlined in the UN Secretary General's latest report on the intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls, some forms of TF VAWG are an extension of existing forms of VAWG e.g. sexual harassment, intimate partner violence, stalking, and trafficking.[25] In some jurisdictions, these could be covered by existing VAWG legislation, as the same protections should apply whether the crime occurred in a digital or a

physical space. Existing laws, however, may not provide adequate protection for more novel forms of TF VAWG, such as the creation and dissemination of non-consensual intimate images or deepfake videos.[26] Comprehensive laws addressing the full spectrum of TF VAWG are critical to ending impunity and ensuring justice, protection and support for victims/survivors. Without these, police may be unprepared to respond effectively to TF VAWG.

National legal frameworks do not always provide a legal basis for clear police interventions. Concepts such as "intimidation" may not be explicitly defined.[27] This leaves police acting on their own discretion, resulting in gaps in protection for women and girls. For example, one investigator may view intimidating online behaviour as potentially criminal; another may dismiss it. When the legal status of some TF VAWG crimes, e.g., intimate image-based abuse, is not stipulated, incidents may be reported by victims but not consistently recorded as offences.[28] Such inconsistencies erode trust in the police.

Some laws focus on the *dissemination* of offensive content, which must be displayed publicly or *transmitted* to constitute a criminal offence. Such provisions create a legal loophole.[29] They do not address instances where perpetrators create or record objectionable content and then threaten to share it, even without publishing it. A threat can cause equally serious psychological harm to women and girls and become a form of sexual exploitation and blackmail.

Legal frameworks may not spell out the roles and responsibilities of private tech companies and law enforcement in responding to TF VAWG. This can make it unclear what tech companies should do (e.g., content moderation or removal) and what law enforcement should do (e.g., request platforms to remove abusive content or share data). This lack of clarity can result in inconsistent, delayed or ineffective responses to complaints by victims/survivors.

Difficulties in identifying and locating perpetrators[30]

Intimate partner violence and coercive control

In intimate partner relationships involving coercive control, geolocation technology and tracking devices are often used to acquire vital information about victims and control them. Unwanted pictures, images and messages sent by abusive partners convey a threat or warning. They may discourage a particular behaviour by the victim, such as calling a family member, friend or the police.[31] Common forms of TF VAWG involving coercive control include call auditing, cyberstalking, telephonic interference, and monitoring with mobile phones, transmitters and video cameras, including within the home.[32] Police can investigate these practices through seizing and inspecting mobile phones, computers and transmitters. Identifying and tracking coercive controlling partners can involve complex investigations and multijurisdictional liaison, however, as offenders often frequently change their employment and residence.

Anonymous perpetration of TF VAWG

Experiencing abuse through an anonymous account online can be very distressing for victims. It is difficult for law enforcement to identify and prosecute individuals who hide behind anonymous or fake accounts, as these accounts are not easily identifiable.[33] They can be quickly discarded and replaced with new anonymous accounts, making techniques such as blocking and muting ineffective.[34] When complaints are filed against perpetrators hiding behind anonymous accounts, police require basic subscriber information from social media platforms to track their identities.[35] Police investigations can be curtailed if online platforms limit data-sharing. Police can also encounter obstacles in identifying where the incident originated and potential secondary perpetration if images are (re)shared. In TF VAWG perpetrated against women in public life, especially, which may include trolling and gendered disinformation, offenders may use anonymizing technology such as a virtual private network (VPN) to hide their IP addresses and locations.[36] They may also hire troll farms as part of a coordinated attack.[37]

Transnational nature of TF VAWG

Diverse legal frameworks and limited coordination and cooperation among States and different jurisdictions all hamper the ability of police to investigate and prosecute offenders for TF VAWG crimes in a timely manner. Perpetrators can operate from any location with internet access, and existing legal frameworks often fail to account for the transnational nature of cyberspace. Law enforcement agencies often need to navigate different national laws and mutual legal assistance treaties to investigate TF VAWG. This can lead to significant delays, especially in cases requiring quick access to data.[38]

Lack of specialized skills, including digital forensic capacity

The perpetration of TF VAWG often involves sophisticated technologies that evolve faster than law enforcement agencies' capabilities. Many police actors are limited in their technical capacity to both collect and understand evidence on offences involving technology.[39] In many countries, training in digital investigation is not incorporated into core policing curriculum.[40] Tools that conceal identity and dark web platforms make it difficult to track perpetrators, especially where investigators have limited forensic tools and capacity. This shortfall is often compounded by a lack of protocols, standard operating procedures and financial resources to oversee the collection, storage and transfer of evidence, including sensitive digital data, so that it is admissible in court. Further, police may not possess skills to communicate the functions of technologies[41] so that prosecutors can determine what charges to bring and present evidence in court that is more readily understood by judges.

Police face an exponential growth in TF VAWG incidents in many countries.[42] Their digital capacities are overstretched, with significant backlogs in the examination and analysis of digital forensic material.[43] As police manage large caseloads, it becomes difficult to develop specialized expertise to identify and investigate TF VAWG, including knowledge of technological advances or understanding of how online abuse can translate into offline violence. A compounding factor can be insufficient coordination between departments with expertise on cybercrimes and those addressing VAWG. Many investigations fail to fully take advantage of both disciplines.

Lack of data on TF VAWG

In many countries, data on general cybercrimes are not disaggregated to capture TF VAWG. Additional data sources may remain untapped, including from platforms and social media companies as well as helplines and other front-line service providers.[44] This is a missed opportunity. Such data could help to provide a more comprehensive picture of the extent, patterns and impact of TF VAWG, and could aid in unmasking anonymous perpetrators. They could also inform the development of new policies and programmes addressing TF VAWG, including awareness-raising and training.

3. Essentials for an effective police response to TF VAWG

Police can take several actions to apply the guiding principles for an effective response to TF VAWG. They should be proactive in deepening their understanding and knowledge of TF VAWG, including its various forms and harm to victims/survivors. They should be able to navigate the rapidly changing legal landscape, stay updated on the latest digital platforms and technologies used in TF VAWG, engage a wide range of stakeholders to address these crimes effectively, and raise community awareness about TF VAWG while encouraging reporting. All these capacities will support prevention and early intervention.

Understanding the legal landscape

Navigating the evolving legal framework around TF VAWG is vital. Police must work within the bounds of national laws that address these crimes, which vary significantly across countries. While specific legislation may already address various forms of TF VAWG, the legal landscape must continuously evolve to keep up with technological advancements. Police must remain up to date on relevant legal frameworks that guide responses, for example, on online hate speech, including radicalization of young people, data protection, and capturing and managing digital evidence.

Where legislation on TF VAWG does not exist, police may consider pivoting to international norms and police good practices that reflect the principles of legality, necessity, proportionality and accountability.

In **Iceland,** adopting the **Act on the Protection of Sexual Privacy and the Act on Stalking (2021)** marked an important step in the legal recognition of TF VAWG and the protection of women and girls. Sharing sexual videos and images without consent is now punishable by up to four years in prison, for example. Threats to share such content may result in up to a year in prison.

To enforce the law, the **Icelandic Police Commissioner** established the **Office for Internet Safety.** It has been instrumental in raising awareness of TF VAWG by:

- Updating police on Internet safety trends, technology-facilitated investigative approaches and emerging digital forensic tools to capture and manage digital evidence;
- Embedding Internet safety and policing in professional and foundational training, including in academy curricula;
- Strengthening criminal justice outreach in responding to TF VAWG;
- Enhancing information on Internet safety, developed through strategic partnerships with a range of private and public stakeholders, and made publicly available.

Capacity-strengthening

Police need ongoing training to remain up to date on the latest digital platforms and technologies used in TF VAWG.[45] Understanding the digital landscape is crucial for effective investigation and prevention. Messaging regarding the severity of TF VAWG and the need for an effective police response should come directly from the top of the organization. Appointing executive or senior police officials as public champions can actively promote awareness and the integration of investigative skills into basic police training and professional development for officers at all levels.[46] The delivery of training needs to be flexible and contextualized, considering the resources, culture and capacities of different police organizations. Cybercrime units should also receive training[47] on identifying and managing specific gender-related digital violence and deepen their understanding of the workings of gender equality and discrimination more broadly.

Guiding principles for an effective police response to TF VAWG

- **Victim/survivor-centred approach:** Cases of TF VAWG are as serious as cases of other forms of VAWG. They must be handled with care, with risks appropriately managed. The principle of non-discrimination in the access to and availability of appropriate and adaptable services should be applied to best support victims/survivors. In investigations, a victim/survivor-centred approach encourages police to draw on other sources of information on the crime, using technical means, so that the burden of evidence-gathering is not placed solely on the victim/survivor.
- **Informed consent:** The victim/survivor should be informed and aware of each step of reporting and investigation. Police must seek the meaningful and consensual participation of victims/survivors,[48] in all their diversity. Victims/survivors should be fully informed of how their confidentiality will be respected, including in the storage and use of digital evidence.
- **Trauma-informed approach:** Police should demonstrate understanding of the real and significant impact of TF VAWG on victims/survivors, and how this violence is part of a continuum of different forms of VAWG that may start, continue or be aggravated by the use of information and communications technology.
- **Address gender bias and do no harm:** Building police capacities to identify unconscious biases and deepen their understanding of TF VAWG and associated harms to victims/survivors can reduce the risk of potential secondary victimization.
- **Being perpetrator-focused:** Maintain a focus on the perpetrator throughout the police response and investigation to understand their behaviour, both on and offline, and hold them accountable. Gathering evidentiary material, including digital evidence, to establish the elements or facts of the case should use all means available, in a timely manner.
- **Intersectionality:** Specific groups of women and girls experience disproportionately high levels of TF VAWG, due to multiple and intersecting forms of discrimination. Police must be culturally sensitive to their needs and have a firm understanding of the context in which they are operating.

Collaboration with civil society organizations offers another way to address the knowledge gap within local police organizations; ideally training should be institutionalized and not ad-hoc.[49] These groups can provide police training on which cases meet legal requirements, advise on image removal or signposts to relevant services, and support awareness-raising on issues related to VAWG.

To help police in the Pacific region respond to technology-facilitated violence, the Pacific Islands Chiefs of Police has created Cyber Safety Pasifika (CSP). It aims to boost cyber safety awareness in vulnerable Pacific communities and improve police skills in cybercrime investigations.

The Australian Federal Police delivers the CSP and trains Pacific police partners on cyber safety awareness and education, cybercrime investigation skills, and cybercrime legislation and policy development.

Professional development is kept simple and user-friendly. Chat groups and messaging boards provide mentorship and remote support. Programme participants in turn guide colleagues on effective and immediate responses to TF VAWG. The CSP also encourages police to actively engage in communities to raise awareness of TF VAWG and avenues of support for victims/survivors.

Photo courtesy of the CPS: 'Training in the Pacific.'

Providing support to victims/survivors

Adopting a victim/survivor-centred, trauma-informed and context-led approach is essential in any police response to TF VAWG.[50] This includes reaching out to platforms to remove abusive content. Support for the deletion of illegal content is critical to the well-being of victims/survivors and helps prevent prolonged harm. Police should also provide victims/survivors with information on protective measures; connect them with other sources of support, such as health and social services; and offer guidance on strengthening/securing their digital presence.[51] They should avoid placing the burden on victims/survivors to respond to the risks created by technological tools.

Some governments and regulators argue for weakening end-to-end encryption to help detect criminal activity, address child sexual abuse material, or enable faster access to evidence for law enforcement. However, weakening encryption can increase gendered-related harms. For many victims/survivors of domestic violence, sexual violence, stalking and trafficking, strong encryption is necessary to maintain private and secure ways for them to contact support services, coordinate escape plans, or document their experiences to preserve evidence for legal action.[52] Encryption can also prevent perpetrators from accessing victims/survivors' communication and information.[53]

Several countries have diversified how victims/survivors can report cases of TF VAWG, through making secure online reporting portals available for those who wish to report incidents.[54]

A digital platform run by the Ministry of the Interior in **France** provides 24/7 support to victims-survivors of cyber harassment[55] allowing them to chat online with police officers specifically trained to respond to these cases. Victims/survivors can obtain support and are accompanied when filing complaints in cases of insults and hate speech, hacking, doxing, non-consensual intimate image-sharing and digital domestic violence, among other forms of TF VAWG. The platform provides:

- Reporting assistance: Victims/survivors can obtain help from a police officer to file a complaint, before being referred to appropriate legal services, local victim support partners, psychologists and legal information centres for comprehensive and personalized care.
- Round-the-clock service provision: The platform is free and accessible 24 hours a day, 7 days a week, from a computer, tablet or smartphone. It is also intended for witnesses, relatives of victims and professionals.
- Trained service providers: Approximately 50 police officers and gendarmes are trained and available to assist victims/survivors with necessary procedures, based on their respective cases.

The **Mauritian** Cybercrime Online Reporting System[56] is a national online system that allows the public to report cybercrimes securely. It provides advice on recognizing and avoiding common cybercrimes on social media. Key elements include:

- Coordinated multisectoral action: The system was set up through collaboration among various stakeholders, including the Ministry of Information Technology, Communication and Innovation; the Computer Emergency Response Team of Mauritius; the Attorney General's Office; the Cyber Crime Unit; the Information and Communication Technologies Authority and the Data Protection Office.
- Awareness of digital safety: The system provides education on different forms of digital violence and concrete tips on prevention and protection from cybercrimes on social media.

The Women and Children Cybercrime Protection Unit[57] is a specialized unit within the **Philippine** National Police's Anti-Cybercrime Group. Established to address TF VAWG, it investigates and prevents cases. The unit focuses on addressing online sexual exploitation of women and children, cyberstalking, sextortion, non-consensual sharing of intimate images, and online grooming and luring. It works closely with local partners, including NGOs and tech platforms, to identify perpetrators and protect victims/survivors. It provides:

- Access to support services: The unit supports victims/survivors to access services, including psychological support;
- Capacity-building: Internal training and skills development help officers provide trauma-informed responses to TF VAWG;
- Assistance in reporting cases of TF VAWG: Support aids victims/survivors in filing cases under relevant laws;
- Awareness-raising: Awareness campaigns are undertaken on various forms of TF VAWG.

Prevention: Awareness-raising and community engagement

Raising awareness about TF VAWG within communities and encouraging reporting supports prevention and early intervention.[58] Transparent communication by law enforcement enhances public trust and awareness, while community education on safe online practices can both foster reporting and support prevention. School-based prevention interventions have proven impactful, as have initiatives that target out-of-school young people, particularly girls, who are highly vulnerable to digital violence.[59] Police should also identify and consult with individuals, groups, communities and professions at greater risk of experiencing TF VAWG,[60] including identifying online platforms and other digital spaces where violence occurs.

The Digital Sex Crime Comprehensive Response Strategy launched by the Seoul Metropolitan Government in the **Republic of Korea** includes a pillar on prevention, specifically, counselling programmes for young perpetrators to prevent recidivism. The curriculum raises awareness of the human rights of children, adolescents and women; addresses stereotypes and biases related to VAWG, including sexual violence; promotes understanding of the importance of empathizing with victims/survivors; and works with perpetrators to establish and practice alternative behaviours.

Multistakeholder partnerships

Addressing TF VAWG requires a comprehensive response involving multiple stakeholders. Police are encouraged to proactively seek and build broad partnerships for prevention-based digital safety. Partners may comprise private and public stakeholders in the tech and social media industries, academia and non-governmental organizations with tech expertise, and women's rights organizations, including those providing front-line support to victims/survivors.[61] Fostering collaboration with other law enforcement agencies is critical.[62]

Through these partnerships, formal information-sharing agreements, led by governments together with tech companies, can support police in investigations. Companies hold critical information and evidence for prosecutions, including on crimes outside the jurisdiction of law enforcement. Clear cooperation frameworks between the

police and tech platforms can support quick and effective action on TF VAWG. Examples of cooperation can include specific portals for law enforcement to request data or its preservation, ask for quick removal of harmful content, or inquire about user profiles, including account information or IP logs.

An example of collaboration to address TF VAWG includes the TAKE IT DOWN Act in the **United States**. It criminalizes the nonconsensual disclosure of intimate images (NDII), whether authentic or digitally generated. Threats involving authentic NDII or digital forgeries are also punishable. It also establishes a rapid takedown process, requiring certain platforms that host user-generated content to remove reported material within 48 hours of receiving a complaint. The TAKE IT DOWN Act expands law enforcement agencies' ability to respond to emerging forms of tech-facilitated harms, but its effective implementation will require further training for police to effectively investigate and support the prosecution of image-based sexual abuse.

The e-Safety Commissioner in **Australia** has partnered with police to develop a comprehensive approach to addressing TF VAWG. This has been particularly important in highlighting how technology-facilitated violence is not a new phenomenon but a more extreme extension of gender-based violence, with women and girls targeted or disproportionately affected, especially by online abuse.

The e-Safety Commissioner advocates for police training to include local magistrates and other justice actors, such as digital forensic teams, to develop a common understanding of TF VAWG across the justice system. The experience has shown that police can be very effective in initial responses to TF VAWG, even with basic digital literacy skills, as long as they are applying a trauma-informed, culturally safe and victim/survivor-centred approach. Since online safety is a global matter, eSafety's International Engagement Team engages with other governments and relevant services, including police, across Asia and the Pacific.

The Violence Against Women and Girls Taskforce in the **United Kingdom** was set up by the National Centre for Violence and Public Protection in 2021 to support a coordinated policing response to VAWG. The taskforce has initiated several actions focused on technology-facilitated and online VAWG.[63] These include:

- Training: The College of Policing developed an e-learning syllabus on digital investigation methods and tools aimed at front-line officers and staff. It includes a dedicated module on investigating technology-facilitated abuse and stalking;
- Collaboration framework: A tech working group was created with the VAWG and Rape and Serious Sexual Offences Taskforce as a platform for collaboration, linking to the Home Office, Crown Prosecution Services, Police Digital Service, other forces and the VAWG Taskforce. The working group provides a platform for police and partners to engage with tech suppliers.

4. Checklist of dos and don'ts for an effective police investigation of TF VAWG

Dos	Don'ts
DO take all reports of TF VAWG seriously, in recognition of the threat, risk and serious harm associated with this type of violence. Practice empathy and ensure that all first responders and investigators understand the principle of "every contact leaves a trace" and a lasting impression – good or bad – on victims/survivors.	**DON'T** minimize harms caused by TF VAWG or blame the victim/survivor for their victimization.
DO ensure the availability of easily accessible online and offline reporting/complaint mechanisms for TF VAWG; prioritize initiatives that inform the public of their existence.	**DON'T** investigate the victim/survivor and their conduct when they have been victimized; be perpetrator focused.
DO consider bringing in a victim/survivor advocate to work with victims/survivors during initial reporting of TF VAWG. This can help create a safe and supportive environment.	**DON'T** ever engage with or interview the victim/survivor in the presence of the suspected abuser and/or his/her surrogates, family members or neighbours.
DO prioritize the victim's/survivor's safety, dignity, privacy and well-being. Share information, tools or other resources, either from your organization or externally, such as details on psychosocial counselling or legal services.	**DON'T** make assumptions that first responders should be the same sex, ethnicity, national origin or religion as the victim/survivor; take your lead from the victim/survivor.
DO remember that victims/survivors of TF VAWG can suffer significant personal and emotional trauma as well as negative impacts on employment and housing, depending on the nature of the crime. Any stressors and sustained losses should be clearly documented in a victim impact statement. Ideally, the statement should set out any evidence that the event was targeted at them specifically, e.g., if the image was sent to their personal account or that of their friends or family.	**DON'T** breach the victim's/survivor's privacy and confidentiality.
DO check if your police organization has a written policy on online investigations of TF VAWG. Be sure that any online investigation has approval of the supervisor and follows written policies and procedures.	**DON'T** make any changes to digital evidence that may be presented in a court of law at a future time.
DO secure and preserve evidence, including digital devices, in TF VAWG cases, and explain to the victim/survivor what you are doing and why, and how downloaded information will be securely stored. Handle and manage the victim's/survivor's data and information obtained or otherwise seen on digital devices with sensitivity and confidentiality.	**DON'T** download and store evidence on your personal device or send it electronically to others.
DO ensure that investigatory searches of the victim's/survivor's digital devices are proportionate, legal and necessary for the defined purpose of the investigation.	**DON'T** seize electronic evidence if you are not formally deemed competent to do so; request assistance as needed. A competent person must be able to present the evidence explaining its relevance.
DO consider all potential evidence and material that could lead to the identification of an offender. This means that anonymous accounts do not automatically close an investigation.	
DO keep a documented record of all actions taken and by whom when handling all evidence in cases of TF VAWG.	

Dos	Don'ts
DO stay connected. Encourage victims/survivors to reach out if any new developments arise, and especially to let you know if a bad actor escalates or continues to engage in contact with the victim/survivor. Staying connected and providing the victim/survivor with appropriate information throughout the process is important, regardless of whether a suspect can be immediately identified.	
DO be an advocate. Consider community outreach and messaging strategies that demonstrate that your organization takes digital abuse as seriously as other potential crimes.	

Acknowledgement

This Brief was prepared by the Ending violence against Women and Girls Section of UN Women based on the guidance set out in the forthcoming *Guide for Police on Addressing Technology-Facilitated Violence against Women and Girls* (UN Women, UNODC and UNDP). The following experts contributed to the development of the Brief: **Amna Baig**, Superintendent of Police, Police Service of Pakistan and Yale University World Fellow with expertise in addressing and preventing TF VAWG; **Gerry Campbell**, former Scotland Yard Detective Chief Superintendent with over thirty years' experience serious crime investigations and international law enforcement; **Mirko Fernandez,** Victim Advocate for the Global Fund Ethics Office in Geneva with expertise in safeguarding and trauma-informed investigations; and **Jane Townsley**, a retired senior police officer from the UK with over thirty years' experience, including as a gender specialist in the field of policing and security, and former Executive Director of the International Association of Women Police.

Endnotes

1 World Bank. 2023. Protecting Women and Girls from Cyber Harassment: A global assessment. Blog posted on 27 November 2023.

2] Jacqueline Hicks, Global evidence on the prevalence and impact of online gender-based violence, Institute of Development Studies, 8 October 2021, p. 2.

3 See the 2024 report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls. A/79/500, para. 17.

4 UN Women and United Nations Office on Drugs and Crime (UNODC). 2025. Femicides in 2024: Global estimates of intimate partner/family member femicides ps.17-18.

5 Between 90 and 95 per cent of all online deepfakes involve non-consensual pornographic images, with approximately 90 per cent of those images depicting women. See the 2024 report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls, para. 23.

6 Zoom-bombing is when an individual joins and disrupts a zoom meeting with inappropriate audio, video or screen sharing content. See https://drexel.edu/it/help/a-z/zoom/zoombombing

7 Doxing is the publication of private and identifiable personal information without permission. It includes situations where confidential information and data, such as phone numbers and home addresses, retrieved by a perpetrator is made public with malicious intent, usually with the insinuation that the victim is soliciting sex. See the 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), para. 36.

8 Gendered disinformation is a strategy to silence women and gender-diverse voices. It is also a form of online gender-based violence in some situations. It is gendered because it targets women and gender nonconforming individuals, because of the gendered nature of the attacks and their gendered impact, and because it reinforces prejudices, bias and structural and systemic barriers that stand in the way of gender equality and gender justice. Gender disinformation aims to portray women as weak, incompetent and sexualized objects, incapable of leadership; to drive women and gender nonconforming persons out of public spaces and places of power; and to silence those who do not comply with gender norms. See the 2023 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/78/228), paras. 10 and 12-13.

9 Baig A., Bhattarai P., Bokum I.M., Corin J., Grajcarová E. 2024. Strengthening Democracy by Reducing Threats to Women in Politics Blavatnik School of Government, University of Oxford, p.48.

10 https://www.arabnews.com/node/2581581/amp

11 The principles outlined in this brief should be read in conjunction with the forthcoming Guide for Police on Addressing Technology-Facilitated Violence against Women and Girls (UN Women, United Nations Office on Drugs and Crime and United Nations Development Programme).

12 Dunn, S. 2022. Addressing Gaps and Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Gender-Based Violence. Expert paper prepared for the expert group meeting in preparation for the sixty-seventh session of the Commission on the Status of Women, p. 5.

13 Ibid., p. 3.

14 Refuge. 2022. Marked as Unsafe: How online platforms are failing domestic abuse survivors, p. 9. Available at https://refuge.org.uk/wp-content/uploads/2022/11/Marked-as-Unsafe-report-FINAL.pdf.

15 Herdale G., K. Duddin and O. Jurasz. 2025. Landscape Review: Policing and technology-facilitated and online violence against women and girls, p. 15. Centre for Protecting Women Online and The Open University.

16 European Institute for Gender Equality. 2022. Combating Cyber Violence against Women and Girls, p.14.

17 See the 2024 report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls. A/79/500, para. 22.

18 Social Development Direct and The Global Partnership. 2023. Technology-facilitated Gender-Based Violence: Preliminary Landscape Analysis p. 40.

19 Curtis, J., and G. Oxburgh. 2023. Understanding Cybercrime on 'Real World' Policing and Law Enforcement. The Police Journal 96(4): 573–592.

20 Addressing Gaps and Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Gender-Based Violence, pp. 3–4.

21 Landscape Review: Policing and technology-facilitated and online violence against women and girls, p.11.

22 Derechos Digitales. 2025. Response to call for inputs on technology-facilitated gender-based violence and its impact on women and girls for the study of the Human Rights Council Advisory Committee on technology-facilitated gender-based violence (HRC resolution 56/19), ps. 11 and 22.

23 Protecting Women and Girls from Cyber Harassment: A global assessment.

24 See the 2023 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/78/288, para. 34.

25 See the 2024 report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls. A/79/500, para. 11.

26 Dunn, S. 2022. Addressing Gaps and Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Gender-Based Violence. Expert paper prepared for the expert group meeting in preparation for the sixty-seventh session of the Commission on the Status of Women, ps. 3-5.

27 Baig A., Bhattarai P., Bokum I.M., Corin J., Grajcarová E. 2024. Strengthening Democracy by Reducing Threats to Women in Politics Blavatnik School of Government, University of Oxford, ps. 51-52.

28 Landscape Review: Policing and technology-facilitated and online violence against women and girls, p.11.

29 Baig A., Bhattarai P., Bokum I.M., Corin J., Grajcarová E. 2024. Strengthening Democracy by Reducing Threats to Women in Politics Blavatnik School of Government, University of Oxford, p.53.

30 While this brief is primarily focused on the use of TF VAWG in the context of intimate partner violence, including through coercive control, and the challenges associated with anony-

mized perpetration, it is important to acknowledge that many other perpetrators not covered by these two categories. These include but are not limited to classmates, work colleagues, and neighbours, who may or may not make efforts to hide their identities while committing TF VAWG.

31 See the forthcoming Guide for Police on Addressing Technology-Facilitated Violence against Women and Girls UN Women, United Nations Office on Drugs and Crime and United Nations Development Programme).

32 Rogers M. M., C. Fisher, P. Ali, P. Allmark and L. Fontes. 2023. Technology-Facilitated Abuse in Intimate Relationships: A scoping review. Trauma Violence Abuse 24(4): 2210–2226.

33 Anonymity and identity shielding | eSafety Commissioner

34 Ibid.

35 Baig A., Bhattarai P., Bokum I.M., Corin J., Grajcarová E. 2024. Strengthening Democracy by Reducing Threats to Women in Politics Blavatnik School of Government, University of Oxford, p.56.

36 United States, Department of Justice. 2023. Technology

37 United States, Department of State. 2023. Gendered Disinformation: Tactics, themes, and trends by foreign malign actors.

38 Coupland, H. n.d. Investigating Cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them, pp. 1–4.

39 Addressing Gaps and Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Gender-Based Violence, p. 4.

40 Landscape Review: Policing and technology-facilitated and online violence against women and girls, p. 31.

41 Addressing Gaps and Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Gender-Based Violence, p. 4.

42 Baig A., Bhattarai P., Bokum I.M., Corin J., Grajcarová E. 2024. Strengthening Democracy by Reducing Threats to Women in Politics Blavatnik School of Government, University of Oxford, p.54.

43 Landscape Review: Policing and technology-facilitated and online violence against women and girls, p. 21.

44 Ibid., p.15.

45 https://www.police1.com/cyber-crime/police-response-to-technology-facilitated-violence

46 Handbook-on-gender-responsive-police-services-en.pdf p. 269

47 https://www.unodc.org/documents/Cybercrime/UNODC-brochure_Comp-3.pdf?v=4.3

48 Child consent is given as part of the investigative process within the legal limits of this consent and the obligation to listen to the child, while placing their safety, protection and best interests at the centre of all decision-making.

49 Majumdar, S. 2020. Police as an Entry Point to End Violence Against Women And Girls – Lessons from civil society organisations funded by the UN Trust Fund to End Violence Against Women and Girls Working paper, p. 23.

50 https://www.police1.com/cyber-crime/police-response-to-technology-facilitated-violence

51 Ibid.

52 https://www.techsafety.org/understanding-encryption

53 Ibid.

54 UN Women. Global Database on Violence against Women and Girls.

55 https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/plateforme-signalement-cyberharcelement

56 https://maucors.govmu.org/maucors/

57 https://www.facebook.com/PNPACGWCCPU/?locale=ka_GE&utm_source=chatgpt.com

58 https://www.police1.com/cyber-crime/police-response-to-technology-facilitated-violence

59 Findings from the "Global Policy Dialogue to Prevent and Eliminate Technology-Facilitated Gender-Based Violence," (UNDP) 19-20 November 2024, Seoul, Republic of Korea.

60 See forthcoming Guide for Police on Addressing Technology-Facilitated Gender-Based Violence against Women and Girls (UN Women, UNODC and UNDP).

61 Landscape Review: Policing and technology-facilitated and online violence against women and girls, p. 33.

62 https://www.police1.com/cyber-crime/police-response-to-technology-facilitated-violence

63 Landscape Review: Policing and technology-facilitated and online violence against women and girls, ps. 26-27.

220 East 42nd Street
New York, New York 10017, USA
Tel: 646-781-4400
www.unwomen.org

UN WOMEN

FOR ALL WOMEN AND GIRLS