SAFER TECH SAFER WORLD

A call for courageous government action to prevent tech-facilitated gender-based violence

ALL IN
GLOBAL LEADERS *for* ENDING GENDER-BASED VIOLENCE

TABLE *of* CONTENTS

Letters From All In Leaders 4

Report Summary 6

Introduction 10

About All In 10
A call to action for government leaders 12

01 Tech is amplifying gender-based violence at unprecedented scale 14

Promise and perils of technology 15
Tech-facilitated gender-based violence 16
Forms of TFGBV 18
Human and collective costs of TFGBV 24
Drivers of TFGBV 26

02 There is growing momentum to address TFGBV 30

Foundations built by civil society movements 32
Governments at the forefront 33
Cross-border coalitions and multilateral action 33
Tech innovations 36
Public awareness and demand for change 39

03 It's time to go All In on safer tech 40

A duty of care to prevent online harm 42
Three pillars for action to address TFGBV 46
Pillar 01: Prevention 48
Pillar 02: Response and Healing 52
Pillar 03: Accountability and Justice 54
Enablers of change 56

Our commitment as All In 58

Acknowledgments 60
Endnotes 62

LETTER *from* ALL IN LEADERS

Each of us stepped up as an All In Global Leader because we refuse to accept that gender-based violence is inevitable. We believe that a world where everyone lives a life of joy, safety, rights and freedom is possible.

This report focuses on a particular form of gender-based violence; violence that is enabled by a phone, computer, device, or screen, supercharged at a new scale and reach. Our concern is not only for the women and girls who are disproportionately harmed by technology-facilitated gender-based violence; but also for current and future generations of young people who are learning and watching, through sheer repetition, that abuse, harm, and misogyny are a normal part of life.

The data are staggering. Among women journalists, activists and human rights defenders, 70% have experienced technology-facilitated gender-based violence, usually with the aim of driving them out of public life. Women parliamentarians are also increasingly targeted. AI-generated child sexual abuse material has increased by 26,385% from 2024 to 2025, with girls comprising 97% of those depicted in AI-generated imagery. And the damage is rippling across our democracies and our collective wellbeing.

This report is fundamentally about rebalancing power. The companies that build these products hold the power to decide what counts as harm, when to intervene, and whether to intervene at all. Safety is currently optional, embedded when convenient and withheld where it is not. Too often, profits take priority over safety, leaving individuals to bear the burden of protecting themselves online. This system must come to an end.

Governments must use the power they have to set guardrails and hold technology companies accountable for people's safety. Governments should mandate a duty of care to place an obligation where the capability to make change sits – with tech companies. Prevention requires safety to be designed into technology from the outset. Response and healing should be available for those already harmed. Accountability should be put in place when the obligation is ignored. There should be transparency in how online harms are addressed. The responsibility to put the safety of people over profits must be standard. We require this of car and food manufacturers, and those industries are safer and more successful for it.

Preventing technology-facilitated gender-based violence is also a matter of human rights. A life free from violence and discrimination is not a privilege of the few; it is the fundamental condition promised by the Universal Declaration of Human Rights to every human being born on this planet. States are obligated under international human rights law to protect against human rights abuses within their jurisdiction by third parties, including by regulating business.

Finally, this report is about courage. As leaders we have negotiated peace and equality at the international level, built global movements, advanced human rights, won a world sporting title, and produced award-winning music, despite repeatedly being told that doing so would be impossible. We have learned that what stands in the way of change is not a lack of knowledge but a lack of will. This is why we are asking governments to legislate as an act of collective courage, and technology leaders and the investors behind them to treat this as an urgent priority and a matter of conscience and responsibility.

When harm is done, there is no neutral position. Not acting makes you part of the *problem*. We know that change is possible. We all have a role to play, and a responsibility to *make it happen*.

TARANA BURKE (Co-Chair, All In)
MARIA FERNANDA ESPINOSA (Co-Chair, All In)
CHARLOTTE BUNCH
DR. DENIS MUKWEGE
PRESIDENT ELLEN JOHNSON SIRLEAF
GABRIELA RAMOS
GEETA RAO GUPTA
H.E. MRS. GRAÇA MACHEL
BARONESS HARRIET HARMAN
JULIE INMAN GRANT PSM
MABEL VAN ORANJE
ROSS TAYLOR
DR. SIMA SAMAR
DR. TRANG NGUYEN
VICTOR MADRIGAL-BORLOZ
VIVIR QUINTANA



REPORT SUMMARY

Technology is supercharging the attitudes, beliefs, and behaviours that have long fuelled gender-based violence (GBV) at an unprecedented speed and scale. Tech-facilitated gender-based violence (TFGBV) is now at a crisis point. TFGBV has significant human impacts, including as a powerful amplifier of offline GBV, and has broad implications for economies, public health, democracy, and peace and security that must motivate government action. TFGBV does not stand apart from the broader crisis of GBV, in which one in three women experience physical or sexual violence in their lifetime.

TFGBV is not an inevitable outcome of technological change. It is a predictable result of choices that value business interests over human rights and profits over safety. It is exacerbated by impunity for individuals who perpetrate harm, and a lack of accountability for technology providers who enable it.

Momentum is now growing to address TFGBV. Years of research and advocacy from women's rights organisations, digital rights activists, survivors, and feminist technologists are resulting in greater public awareness, growing national regulation, and stronger global frameworks. Progress is real, but uneven and insufficient to meet the scale of the problem.

This report challenges governments to show the collective courage to rebalance the power and systems that have fuelled TFGBV for too long. It's time to go All In on safer tech.



REPORT SUMMARY

Governments need to disrupt the system by mandating a duty of care requiring the tech sector to build safety into the design, development, and deployment of technology from the outset, rather than as an afterthought. This is a fundamental shift in responsibility: away from individuals absorbing harm, onto the institutions with the power and responsibility to prevent it.

To address TFGBV, All In calls on governments to implement this duty of care across three pillars:

Prevention

- Shift from reactive to proactive approaches, by mandating Safety by Design
- Close legal gaps on TFGBV
- Embed digital literacy, inclusion, and norms change into national programs

Response and Healing

- Require accessible, trauma-informed reporting mechanisms for TFGBV
- Ensure comprehensive, survivor-centered support services, integrated into national GBV response systems

Accountability and Justice

- Hold technology platforms and perpetrators to account through strong compliance and enforcement
- Ensure justice systems are equipped to deliver for survivors of TFGBV

These actions must be rights-based, survivor-centred, adapted to local contexts. They must take a life course and approach, and be implemented through multistakeholder partnerships across government, industry, and civil society.

Governments must use all tools at their disposal to meet this challenge. This includes prioritising resourcing for effective and robust implementation and enforcement; building the capacity of and engaging survivor-led and women's rights organisations; collaborating through global and regional governance mechanisms; and investing in evidence generation to better understand this evolving issue and its solutions.

To drive the courageous, collective government action needed to address TFGBV, All In is using our platform to mobilise government commitments, amplify the GBV and digital rights ecosystems, and engage new sectors and partners for safer tech, including investors and shareholders. Together, we can build a digital world that's safe, enabling, and joyous for all women and girls.

ABOUT ALL IN

All In: Global Leaders for Ending Gender-Based Violence brings together eminent leaders across sectors – former heads of state, Nobel Laureates, survivor advocates, government leaders, human rights activists, elite athletes and cultural figures – united by one bold premise: gender-based violence (GBV) is solvable. From decades of research and practice, we know what works to prevent GBV. What's missing is the political will, investments, and coordinated leadership to implement solutions at scale. All In Global Leaders have come together to fill this gap between what we know and what we do, using our collective influence to make ending GBV a priority for leaders across countries and sectors.

"For too long, women and girls have been told that online abuse is simply the price of participating in public life. It isn't. Survivors should not have to carry the burden of staying safe online while powerful institutions fail to act.

It's time to shift the burden of safety onto the those with the power to prevent harm. Governments and the technology sector have both the responsibility and the opportunity to build digital spaces where everyone can participate safely, freely and with dignity."

Tarana Burke
All In Co-Chair

INTRODUCTION

A CALL TO ACTION *for* GOVERNMENT LEADERS

All In has chosen "Technology and Gender-Based Violence" as its inaugural thematic priority because TFGBV is a rapidly growing form of violence with significant human impacts, including as a powerful amplifier of offline GBV. TFGBV does not stand apart from the broader crisis of GBV, in which one in three women experience physical or sexual violence in their lifetime. It has implications across our economies, public health, and democracies. It is also an issue squarely within our collective capacity to address.

There are two groups of leaders whose decisions and choices shape the digital world: governments, who set the rules and standards, hold enforcement power, and control national budgets; and the tech sector, whose design choices, business models, and governance either enable or prevent harm. These are the leaders All In seeks to influence.

This report calls on government leaders to use laws, regulations, resources, and political leadership to set and implement a clear standard for safe digital spaces. It focuses on addressing TFGBV, while drawing on the evidence and work of the broader movement to end GBV, protect digital rights, and end online harms. This report is not intended to be exhaustive of all measures needed to end TFGBV but instead focuses on high-impact actions that governments must take at a system level to meet this crisis with the urgency it requires.

All In's first phase on this theme focuses on governments, advocating for regulation and legislation to set and implement basic standards of safety in digital spaces. The second phase, launching in 2027, will focus on catalysing action across the tech sector, including by influencing shareholders and investors, to create safe digital spaces for all, with a focus on ending TFGBV in all its forms.



01

TECH IS AMPLIFYING GENDER-BASED VIOLENCE AT UNPRECEDENTED SCALE

PROMISE AND PERILS *of* TECHNOLOGY

Technology has immense power as a force for good. It has improved healthcare outcomes, driven economic growth, helped mobilise movements against oppression and human rights abuses, and advanced progress towards achieving the Sustainable Development Goals. Technology is a vital part of how we work, learn, and build community every day.

For many women and girls, technology has been transformative. It has brought new economic and educational opportunities, enabled connection, and helped build movements across borders. Tech innovations are strengthening the GBV prevention and response field: digital tools can connect GBV survivors to essential support and information, support case management for survivors of violence, and enable scale up of social norms interventions to prevent GBV.

This same power, left unchecked, is being misused to cause harm at scale.

Online harms are widescale and interlocking. One in four children experience online sexual exploitation before the age of 18.[1] Exposure to cyberbullying, self-harm content, and unrealistic body standards is widespread, with consequences on mental and physical health.[2] Boys and young men are increasingly targeted with content that normalises misogynistic attitudes and behaviours, fuels gender-based violence and violent extremism, and harms their own wellbeing.[3,4] And LGBTQI+ people face heightened online harassment, particularly in countries where same-sex relationships are criminalised.[5] Regardless of identity, geography, and ideology, everyone is increasingly impacted by online harassment and abuse.

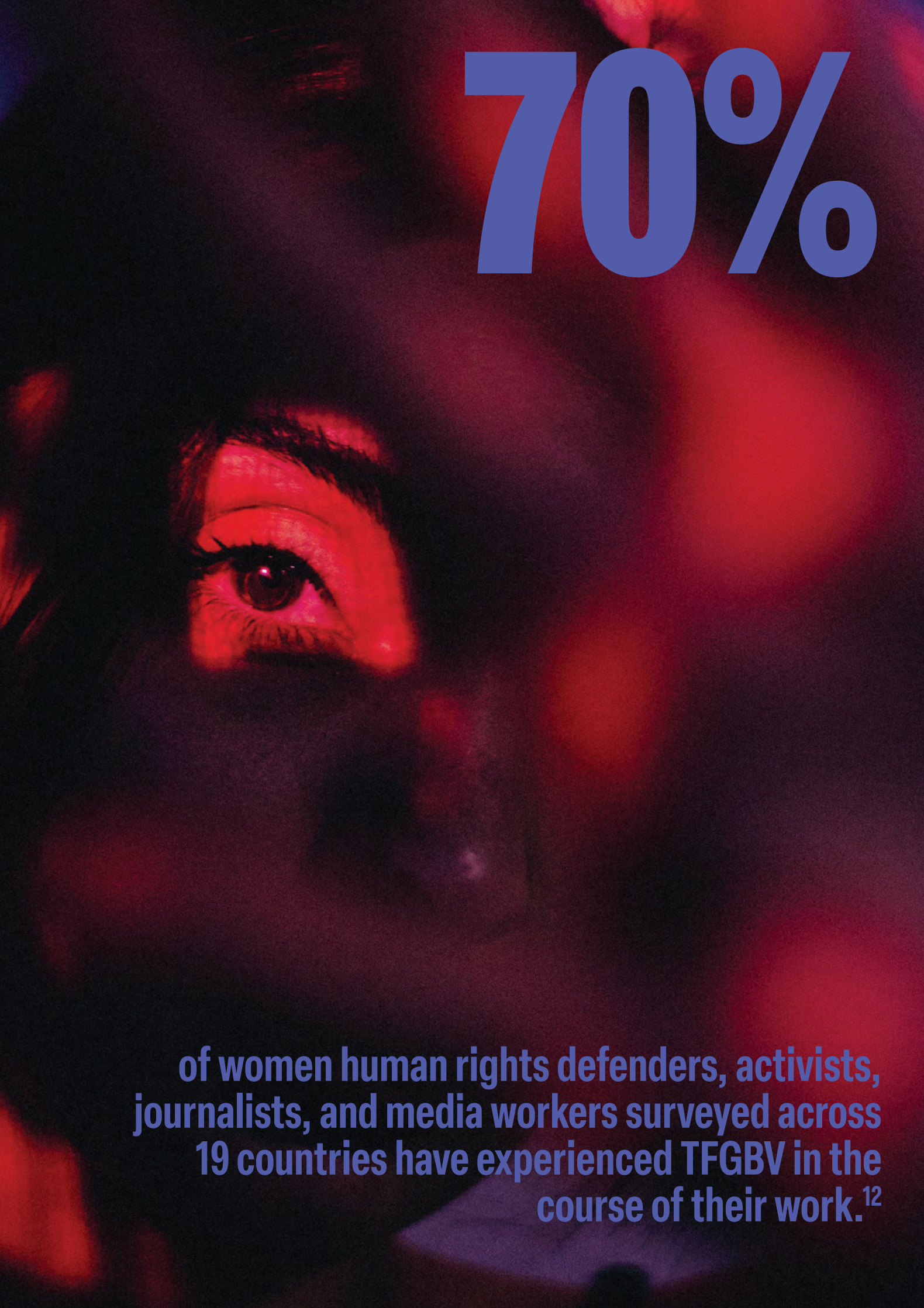
TECHNOLOGY FACILIATED GENDER-BASED VIOLENCE*

Women, girls, and gender-diverse people are particularly targeted by TFGBV, which can include online harassment, abuse, coercion, and exploitation. **TFGBV is at a crisis point.** Global and regional estimates of TFGBV prevalence are high, with estimates reflecting variations in contexts, TFGBV definitions, and widespread underreporting.[6] Some studies estimate that nearly 60% of women and girls have experienced some form of online harm.[7]

Women who face intersecting forms of discrimination face a higher burden of TFGBV, including young women and girls,[8] LGBTQI+ people,[9] women with disabilities,[10] and women of diverse racial and ethnic backgrounds.[11] Women in public life, including politicians, face a particularly high burden of TFGBV: 70% of women human rights defenders, activists, journalists, and media workers surveyed across 19 countries have experienced TFGBV in the course of their work.[12]



*An act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media against a person on the basis of gender.[13]



70%

of women human rights defenders, activists, journalists, and media workers surveyed across 19 countries have experienced TFGBV in the course of their work.[12]

FORMS *of* TFGBV

Over 40 distinct forms of TFGBV have been documented,[14] with new forms continuously emerging as generative AI and other technologies rapidly evolve and create new avenues for harm. These range from the exacerbation of existing forms of violence, like sexual harassment and coercive control, to new forms of violence only made possible by technology, like synthetic image-based abuse and violence facilitated by AI chatbots.[15] No platform or technology is immune: social media, gaming, AI, messaging, smartphones, and location tracking devices have all been weaponised for TFGBV.

TFGBV is part of a continuum of violence. As tech proliferates in our daily lives, the line between on and offline GBV is increasingly blurred; online abuse reinforces and extends into offline violence and vice versa. Abusive male partners are increasingly using digital tools to control and stalk women.[16] Intimate images shared without consent have led to physical violence and so-called "honour killings."[17] Among women journalists and media workers, 42% experienced offline harm such as physical assault and stalking triggered by online violence in 2025 – more than double the rate in 2020.[18]


SURVEILLANCE
DEEPFAKES
STALKING
HATE SPEECH
VIOLENT THREATS
IMPERSONATION
GENDERED DISINFORMATION
ASTROTURFING
DOXXING
CYBER-HARASSMENT
IMAGE-BASED ABUSE
HACKING



SPOTLIGHT ON IMAGE-BASED ABUSE

Sharing or threat of sharing images without consent of the person shown to coerce, threaten, harass, humiliate, distress, objectify or abuse them. Deepfakes and non-consensual intimate imagery (NCII) are forms of image-based abuse.[19]

Examples:

- Almost a hundred 'nudify' applications, whose primary function is to strip clothing from photographs of real people, are available on mainstream app stores.[20]
- There was a **550% increase** in the number of deepfake videos online from 2019 to 2023. Deepfake pornography makes up 98% of all deepfake videos online, and 99% of individuals targeted are women.[21]
- A study of Pakistani women found a wide range of images that women considered intimate and harmful – from showing a woman without a hijab, singing or dancing in public, in her bedroom, or expressing a political opinion. Definitions of what makes an image "intimate" vary across cultures, making **consent-based definitions** essential to categorising and understanding image-based abuse.[22]



SPOTLIGHT ON GENDERED DISINFORMATION

Use of false or misleading gender and sex-based narratives, often with some degree of coordination, aimed at deterring and discrediting the voices, experiences and participation of women, girls, and gender diverse persons in the public sphere.[23, 24]

Examples:

- Gendered disinformation is strategically used by both state and non-state actors to target women politicians, journalists, and human rights defenders with the aim of silencing them, portraying them as unfit for leadership, and discouraging other women from pursuing public roles.[25]

- **This can have a chilling effect.** A survey across 119 countries found that almost a quarter (23.8%) of women human rights defenders, activists and journalists said that they had experienced AI-assisted online violence; 41% said online violence has caused them to self-censor on social media.[26]

- TFGBV is shaping the choices and behaviours of young women and girls. A survey across 26 countries found that one in four girls felt less confident to share their views and one in five stopped engaging in politics or current affairs as a result of disinformation online.[27]

SPOTLIGHT ON ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Children and youth experience online harassment, cyberbullying, grooming, and financial and sadistic sextortion. They are also exposed to child sexual abuse material (CSAM) and groomed for its production. Girls are overwhelmingly represented in CSAM and other forms of online child sexual exploitation and abuse, reflecting a gendered dynamic. However, gendered patterns vary by threat type: adolescent boys are more targeted for financial sextortion.[28] There are many shared drivers, impacts, and solutions for addressing TFGBV and online child sexual exploitation and abuse.

Examples:

- A global monitoring organisation found that **AI-generated child sexual abuse videos increased by 26,385%** from 2024 to 2025 alone. Girls remain overwhelmingly targeted, comprising 97% of illegal AI-generated images assessed.[29]

- A global survey across 31 countries found that **more than half of girls have been harassed and abused online,** and one in four feel physically unsafe as a result.[30]

- The Out of the Shadows Index assessed legislation across 60 countries, finding that only 38 criminalise online grooming and nearly two-thirds are not holding internet service providers accountable for reporting suspected CSAM.[31]

HUMAN AND COLLECTIVE COSTS *of* TFGBV

TFGBV is a human rights violation that impacts all facets of life. For individual survivors, the consequences of TFGBV are widespread and long-lasting. It can leave women and girls with low self-esteem, fear, and poor health, as well as post-traumatic stress disorder, anxiety, and/or depression.[32,33] Survivors may withdraw from online spaces or miss work to stay safe, reducing income and economic participation. In severe cases, survivors may need to relocate to avoid physical harm, often at great cost to their livelihood, stability, and families.[34]

The harm is also collective. The consequences of TFGBV are not felt by survivors alone; they are costs borne by all - families, communities, and societies – with vast ripple effects.

Economies

Governments and taxpayers absorb the price of TFGBV through legal and healthcare costs, lost income and labor, and reduced quality of life.

- In 2021, TFGBV was estimated to cost European Union countries between €49 to €89.3 billion annually.[35]

Democracy

When women in public life are targeted, silenced, and self-censor due to online abuse, political discourse and civic spaces are weakened.

- An analysis of 10 million tweets during Brazil's 2022 election found that female candidates reduced their online activity following misogynistic attacks, evidence that online abuse silences political participation.[36]

Peace and Security

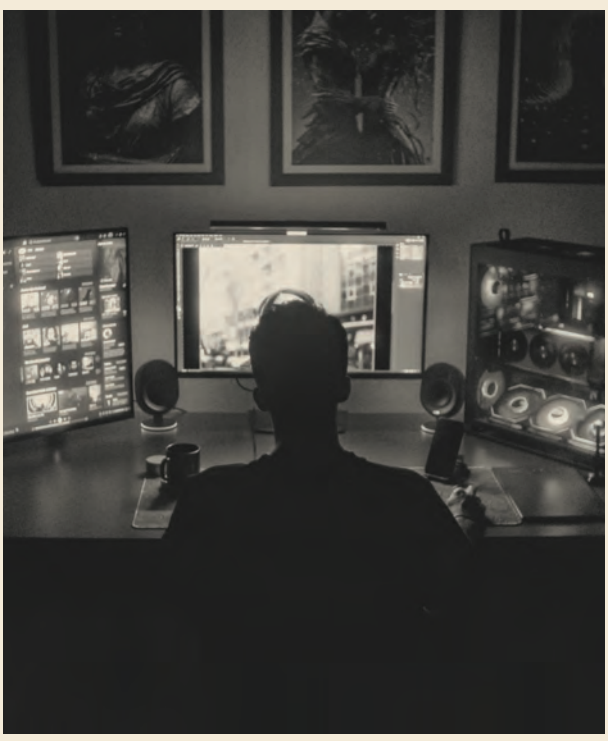
TFGBV is both a tool of and fueled by conflict, directly undermining peace processes and feeding cycles of violence. Evidence continues to emerge linking online misogyny and TFGBV with violent extremism.

- Men and boys who support GBV are up to three times more likely to support violent extremism – a pattern found across studies from Indonesia, Bangladesh, the Philippines, Libya, and the UK.[37]
- In Sudan, since the outbreak of war in 2023, TFGBV (including doxxing, image manipulation, and AI-generated sexual deepfakes) has been used by conflict actors to silence women activists and journalists, and in one case to publicly incite conflict-related sexual violence.[38]

DRIVERS *of* TFGBV

Like all forms of GBV, TFGBV is structural and systemic at its core, rooted in gender inequality and patriarchal norms. Tech is supercharging these norms and inequalities, amplifying the attitudes, beliefs, and behaviours that have long fuelled GBV at unprecedented scale, speed, and anonymity.

Deep-rooted systems of oppression and discrimination are reproduced in technology design, shaping women's and girls' experiences on technology, their access to it, and their participation in digital life. These biases and inequalities are baked into tech's design – women hold only 29% of C-Suite tech positions[39] and only 30% of AI roles today,[40] and gender biases are being trained directly into large language models.[41] A lack of regional, cultural, and linguistic diversity further reproduces inequalities, resulting in gaps in safety and accessibility that can be particularly acute for marginalised groups.

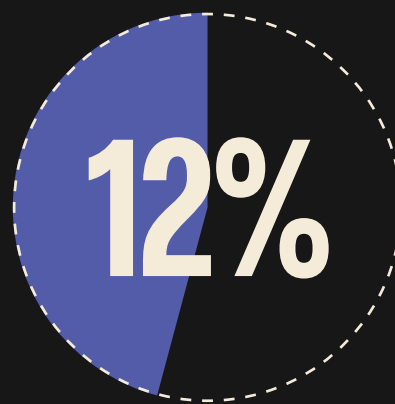


Tech business models compound the problem. When platforms measure success by engagement and rely on engagement-based advertisement revenue, outrage is rewarded over safety and algorithms amplify content most likely to provoke. Commercial ecosystems are being built on generating and sharing TFGBV: for example, in Italy and Spain, researchers documented a sophisticated, monetised TFGBV infrastructure where non-consensual intimate imagery and "nudify" bots are sold and shared across platforms for profit.[42]

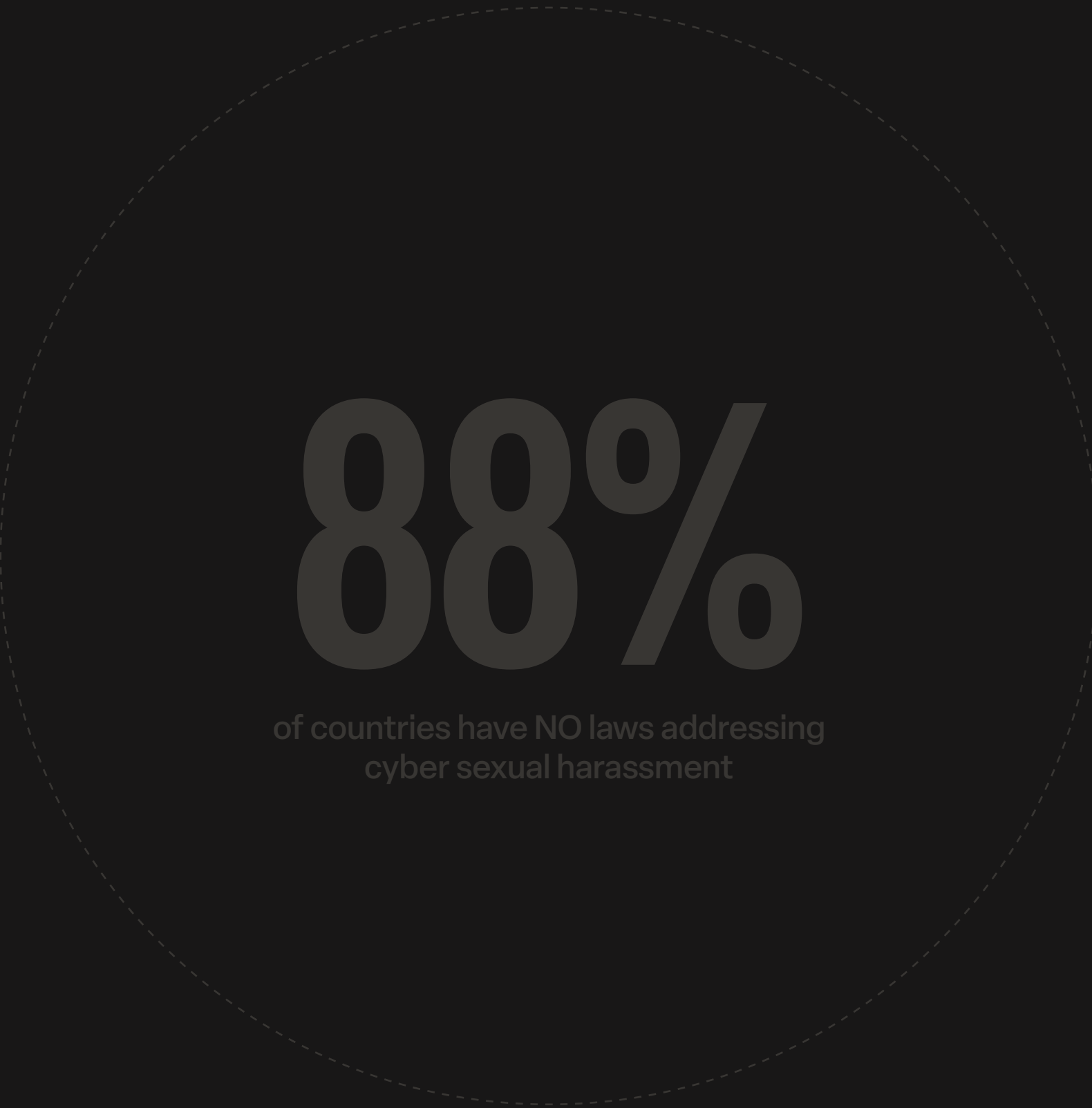
Men and boys are the primary perpetrators of TFGBV. At the same time, technology is facilitating the mainstreaming of misogyny via the so-called "manosphere." This growing ecosystem exploits boys and young men's anxieties and vulnerabilities, manipulates their need for belonging, and builds community out of manufactured grievances.[43] Algorithmic amplification, recommender systems, and other tech features accelerate exposure to this harmful content and reward its creators, moving the rhetoric and beliefs that fuel GBV from fringe online spaces into mainstream public and political discourse.[44] A recent study of young men across the UK, Australia, and the United States found that 63% regularly engage with "masculinity influencers", and those who do are more likely to report psychological distress and hold negative views of women's empowerment.[45]

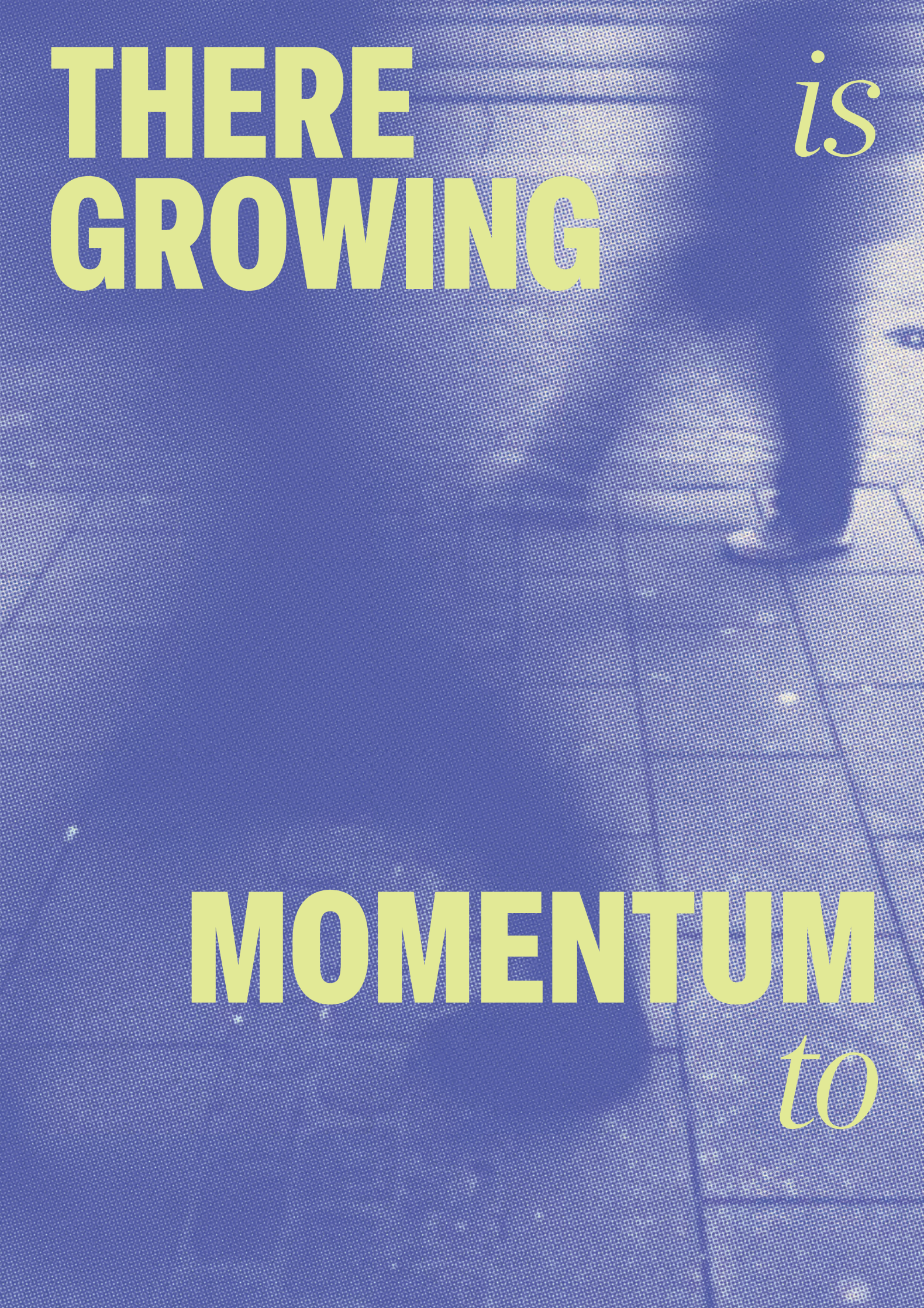
Tech platforms have become a strategic tool for anti-rights actors, offering new and sophisticated ways to organise and attempt to discredit feminist leaders, human rights defenders, journalists, movements, and those challenging power. Perpetrators are no longer only partners or people known to survivors, but opportunists, misogynistic networks, governments, and politically motivated groups who hide behind screens and use gendered narratives to sow division, silence dissent, fuel hostility, and shift public attitudes. The dual rise of TFGBV and the global backlash against gender equality is not a coincidence.

Governments hold the key in setting the rules of the digital road, but too few have taken action. Fewer than 12% of countries have laws addressing cyber sexual harassment;[46] and while 55 countries have gender and AI frameworks, only 24 show evidence of implementation.[47]



Voluntary industry commitments and self-regulation are welcome first steps, but can only go so far to address harm that spreads quickly across tools and platforms. Legal and governance fragmentation creates accountability and compliance loopholes across jurisdictions.[48] These gaps are not insolvable. Governments around the world are already choosing differently, showing what's possible when leaders prioritise tech safety.


88%
of countries have NO laws addressing
cyber sexual harassment


THERE
GROWING
is
MOMENTUM
to

02

We are in a global moment of opportunity to address the crisis of TFGBV. Rising public awareness is meeting years of research and advocacy, growing global and regional normative frameworks, and building momentum for cross-sector action. Progress is real, but uneven and insufficient to meet the scale of the problem. TFGBV is solvable; our toolkit for doing so is growing and urgently requires action and investment.

ADDRESS TFGBV

FOUNDATIONS BUILT *by* CIVIL SOCIETY MOVEMENTS

Decades of research, advocacy, and practice by the GBV and digital rights sectors have made today's progress possible. Women's rights organisations and survivors raised the alarm on TFGBV, working locally and globally to document its manifestations, research its impacts, and lead advocacy for context-responsive solutions. Feminist technologists have led the way in conceptualising and building digital spaces that prioritise safety and centre gender equality in their design, challenging prevalent norms of "move fast and break things" and "scale at all costs" borne out of a male-dominated Silicon Valley.

For example:

- The Feminist Principles of the Internet offer a framework for advocates, researchers, and policymakers for understanding and shaping technologies, covering issues such as access, online violence, privacy, data, and governance.

- The TFGBV Shared Research Agenda brought together researchers, policymakers, funders, and civil society to identify shared priority areas for strengthening TFGBV research and filling evidence gaps.[49]

- Réseau des Femmes Leaders pour le Développement tracks TFGBV incidents and legal developments across Africa through a network of focal points and local organisations, informing advocacy with localised, updated data.

GOVERNMENTS AT THE FOREFRONT

Governments have the opportunity and responsibility to set and implement the standards for a safe digital world that protects and upholds human rights. A growing number of countries at the frontier are enacting laws and regulations that hold both perpetrators and the tech sector accountable, providing models for other countries to follow suit and creating ripple effects across tech globally.

For Example:

- European Union: The Digital Services Act (DSA) recognises GBV as a systemic risk that very large platforms must identify, assess and mitigate, positioning TFGBV as a matter of platform governance.[50] The EU's AI Act was also recently amended to ban nudification apps.[51]
- Brazil: Presidential Decree No. 12,976 establishes guidelines for preventing and responding to TFGBV and introduces stronger platform responsibilities, including rapid removal of NCII and dedicated reporting channels. This decree builds on the 2014 Marco Civil da Internet and a criminal code amendment penalising the use of AI to later images and videos of women.

CROSS-BORDER COALITIONS *&* MULTILATERAL ACTION

TFGBV is a global issue that demands global responses. Because tech platforms are borderless, national legislation alone is not sufficient. Global and regional coordination and governance frameworks are critical to building universal standards of accountability. The last five to ten years have seen growing partnerships and coalitions to set global norms, share solutions, and raise the profile of TFGBV as an urgent human rights issue.

For Example:

- The Global Partnership for Action on Gender-Based Online Harassment and Abuse brings together 21 governments and a multi-stakeholder Advisory Group to strengthen coordinated action on TFGBV through research, knowledge-sharing, and policy development. The Partnership has called for urgent action on NCII based on model legislation.
- The Global Online Safety Regulators Network (GOSRN) brings together independent online safety regulators from nine countries to strengthen international cooperation and coherence on addressing online harms. The Online Safety Regulatory Index collates Network members' approaches to online safety regulation.

Global and regional multilateral frameworks are increasingly recognising TFGBV and calling for prevention and accountability, including:[52]

Convention on the Elimination of All Forms of Discrimination against Women, General Recommendation No. 35 (2017)	Recognises that GBV occurs in online and digital environments. Expands State obligations to include technology-mediated settings in prevention and response efforts.
UNESCO Recommendations on the Ethics of Artificial Intelligence (2021)	First global standard on AI ethics. Recommends States take steps to avoid violence of women and girls in the online domain, and ensure that gender stereotyping and discriminatory biases are not translated into AI systems.
GREVIO General Recommendation No. 1 on the digital dimension of violence against women (2021)	Extends interpretation of the Istanbul Convention to explicitly include the "digital dimension of violence against women."
ASEAN Declaration on the Elimination of Violence Against Women and Elimination of Violence Against Children (2021)	Recognises that violence against women and children can happen in cyberspace. The ASEAN Regional Plan of Action on the Elimination of Violence Against Women further calls on Member States to review and strengthen national laws to address emerging forms of violence against women, including sexual violence facilitated through digital technologies.
Commission on the Status of Women (CSW67) Agreed Conclusions (2023)	First UN intergovernmental agreed language on TFGBV: "violence against women and girls that occurs or is amplified by the use of technology." Calls for comprehensive preventive and eliminatory measures.

UN Convention against Cybercrime (2024)	First global legal framework to combat cybercrime. Calls for the criminalisation of non-consensual dissemination of intimate images and supports cross-border collaboration and digital law enforcement coordination.
Global Digital Compact (2024)	Includes elimination of sexual and gender-based violence that occurs or is amplified by the use of technology as a core principle, and emphasises the need for gender mainstreaming in digital policy.
African Union Convention on Ending Violence Against Women and Girls (2024)	Recognises digital spaces as an emerging context for GBV and establishes legally binding obligations for States to address violence against women and girls on online platforms.
EU Directive 2024/1385 on combating violence against women and domestic violence (2024)	Criminalises across the EU the non-consensual sharing of intimate images (real or manipulated), cyberstalking, cyberharassment, and cyber incitement to hatred or violence.
Council of Europe Recommendation on Accountability for Technology Facilitated Violence against Women and Girls (2026)	First international legal instrument dedicated to accountability for tech-facilitated violence against women and girls, calling for comprehensive measures on prevention, legislation, survivor protection and support, platform accountability, data collection, and multi-stakeholder cooperation.

TECH INNOVATIONS

Beyond government-focused efforts, a growing number of tech companies are taking meaningful steps to proactively prevent and respond to TFGBV. Feminist technologists and Trust & Safety professionals are leading the way to innovate on safety measures that prevent and respond to online harms, often advocating for the prioritisation of safety within their companies. Regulatory pressure, civil society advocacy, and survivor campaigning have underpinned this work, demonstrating why government action to set the standard remains critical.

Select Examples:

- The Safety Showcase: Reimagine Gender in Technology is a multi-stakeholder initiative spotlighting safe, ethical and gender-responsive tech.[53] Finalists have included NOOR AI, an AI-powered platform developed in Pakistan supporting women and girls with disabilities experiencing TFGBV, and Zuzi AI, a multilingual, trauma-informed chatbot developed in South Africa that provides survivors of GBV with legal information, emotional support, and health guidance.

- Tech industry actors are working with organisations and tools like The Tech Coalition's Lantern platform to improve cross-sector collaboration on online harms. Through Lantern, companies can securely share signals with each other when online child sexual exploitation and abuse is detected to help other companies recognise this content, take action, and stop its spread.



90%

of UK adults are concerned about deepfakes and their potential to enable abuse.[56]

80%

of Americans believe the government should maintain rules for AI safety and data security, even if it slows AI development.[58]

57%

of American adults view societal risks from AI as high and want greater control over how AI is used.[55]

53%

of adults say AI makes them nervous.[54]

PUBLIC AWARENESS AND DEMAND *for* CHANGE

Public demand for change is also driving this momentum. Polling data from around the world shows a rising awareness of online harms and wariness of technological advancements like artificial intelligence. According to a 30-country poll, 53% of adults say AI makes them nervous.[54] Some 57% of American adults view societal risks from AI as high and want greater control over how AI is used,[55] and 90% of UK adults are concerned about deepfakes and their potential to enable abuse.[56]

Advocacy and litigation are beginning to chip away at the perceived invincibility of tech. Issues like child sexual exploitation and abuse and the economic and environmental impacts of data centres are finding traction across political ideologies. Civil society campaigns are raising awareness of digital risks and rights, and building public demand for accountability. High-profile survivors of TFGBV are sharing their stories and turning to civil and public interest lawsuits to find justice and accountability. Litigation is finding success, holding Big Tech accountable for harms to young people's mental health and for enabling child sexual exploitation.[57]

The public is calling on governments to prioritise tech safety: 80% of Americans believe the government should maintain rules for AI safety and data security, even if it slows AI development.[58] At the same time, there is mixed trust in governments to regulate tech: about half of adults in global surveys trust their governments to regulate AI responsibly.[59] This gap between demand and government action is an urgent call for governments to act decisively, giving safety and accountability equal weight as growth and innovation when developing AI and tech policy.

IT'S TIME TO GO

This report challenges governments to show the collective courage to rebalance the power and systems that have fuelled TFGBV for too long.

TFGBV is not inevitable. It is a predictable result of choices that value business interests over human rights, and profits over safety. TFGBV is not only a problem of a few bad actors perpetrating harm, but a monetised ecosystem that must be held accountable for enabling harm at scale.



03

Ending TFGBV demands governments go All In on using every tool at their disposal to end impunity, hold perpetrators and the tech sector accountable, support survivors, and foster digital spaces where safety is fundamental, not optional. It is the responsibility of governments to ensure that the choices of a few private individuals and companies alone do not shape global digital spaces for us all.

Together, we can stop the worldwide web from being used as a worldwide weapon.

ALL IN ON SAFER TECH

A DUTY *of* CARE TO PREVENT ONLINE HARMS

We call on governments to rise to this challenge by mandating a duty of care requiring the tech sector to ensure safety is continuously embedded into the design, development, and deployment of technology. This is a fundamental shift in responsibility: away from individuals absorbing harm, onto the tech sector to proactively prevent harms and protect human rights from the outset, rather than after harms have occurred.

This is a shared duty. Governments and the tech sector must both be All In.

- Governments must set the standards for safe digital spaces through laws, regulations, and enforcement. By mandating the tech sector to hard-wire safety into product design and delivery, governments can create a baseline and hold companies to it.

- The tech sector must ensure their products, tools, and services do no harm. This includes holding themselves accountable to governments and users and addressing harm when it occurs, realising their responsibility is not only to a bottom line but to ensuring their platforms do not facilitate abuse.

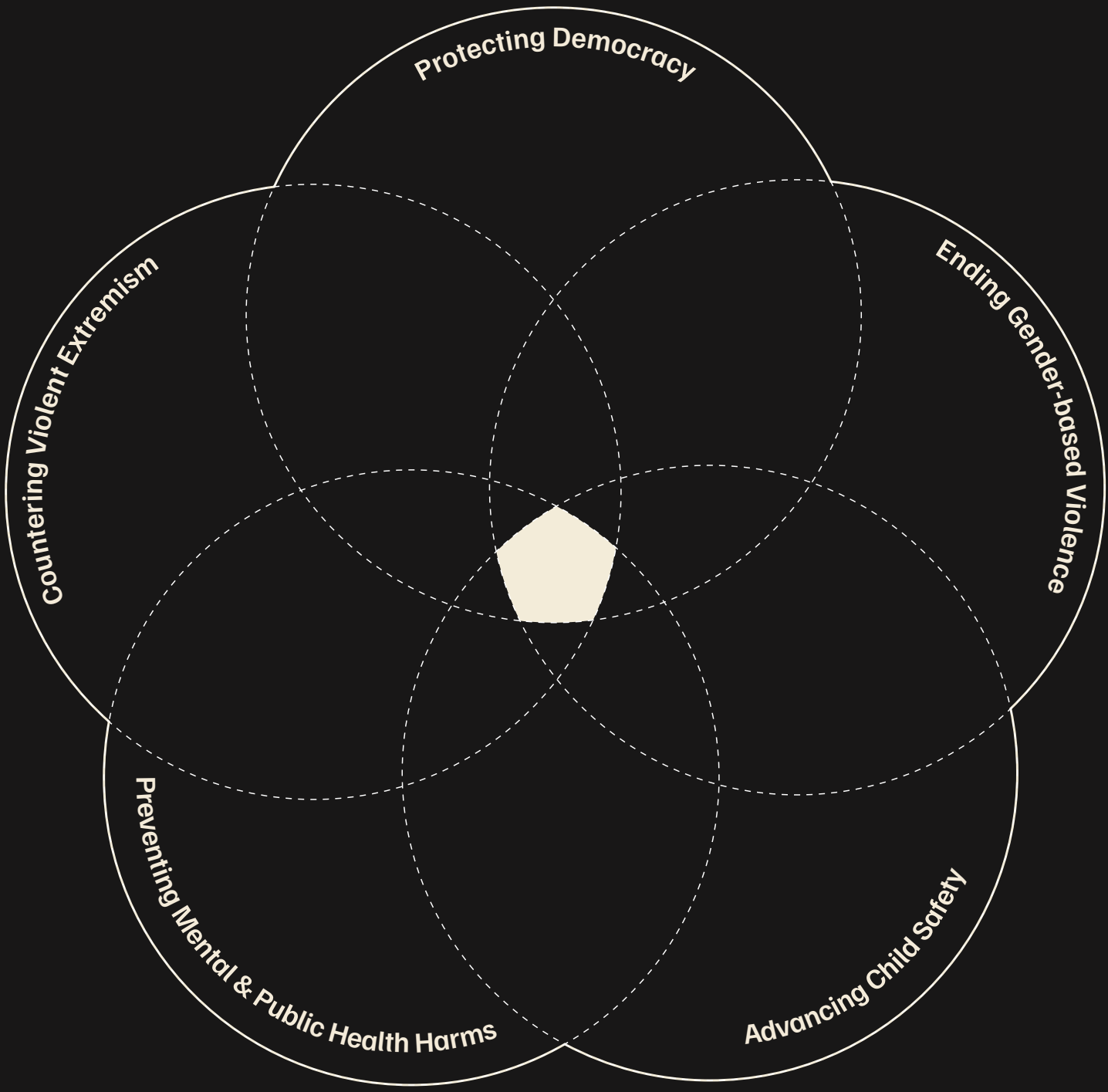
An effective duty of care must go beyond commitments to implementation. Legislation, regulation, oversight, and enforcement mechanisms must be sustainably resourced and given sufficient authority to hold perpetrators and tech companies to account. To meaningfully address TFGBV, this duty of care must specifically recognise gendered harms and draw on the expertise of GBV research, practice, and feminist movements to inform rights-based, survivor-centred policy and design decisions.

Julie Inman Grant
Australia's eSafety Comissioner and All In Thematic Leader

"Industry's faltering inertia on critical online and AI harms proves we've reached the limits of voluntary action. We need a mandated pathway, with *safety by design* as its foundation, to make technology platforms accountable and liable for the safety of the people they profit from. This important work is underway across several countries. All forms of technology should be tools of expression and collaboration, not weapons of gendered violence."

Duties of care are not new and exist across industries. From car seatbelts to food safety inspections, and pharmaceuticals – **regulations and policies across sectors realise a legal and moral obligation to prevent foreseeable harm.** These have been most effective when regulation is coupled with strong compliance and enforcement measures. This call for a duty of care is grounded in human rights frameworks and basic consumer protections, such as the UN Guiding Principles on Business and Human Rights, which establish a State responsibility to protect and a corporate responsibility to respect human rights in business operations.[60]

Fulfilling this duty of care would be catalytic, with the potential to have multiplier effects across intersecting and urgent challenges facing the world today. From ending TFGBV and online child sexual exploitation and abuse, to preventing mental and public health harms, countering violent extremism, and protecting democracy – **creating safe digital spaces is an investment in national and global resilience, security, and stability.**



Safer Tech is a central policy ask across these interconnected movements

THREE PILLARS *for* ACTION TO ADDRESS TFGBV

A duty of care can only be as strong as the education, support, compliance and enforcement behind it. All In calls on governments to operationalise this duty across three pillars to address TFGBV:

Prevention

Shift from reactive to proactive approaches to prevent TFGBV from the outset, including by mandating Safety by Design, closing legal gaps, and driving education and norm change.

Response and Healing

Ensure access to comprehensive, survivor-centered support services and reporting mechanisms when TFGBV occurs, to support survivor healing and wellbeing on and off tech platforms.

Accountability and Justice

Hold technology platforms and perpetrators to account through compliance, enforcement, and strengthening civil and criminal justice system responses to TFGBV.

The following guiding principles should guide all government actions in addressing TFGBV:

- **Rights-based:** Actions must respect and promote human and civil rights and uphold the dignity, empowerment, and autonomy of individuals, including the right to privacy. Governments must hold themselves to human rights standards and principles.

- **Survivor-centered:** Actions must be trauma-informed and put survivor rights, dignity, and respect at the forefront. Survivors must be meaningfully included in consultations and decision-making processes, and care must be taken to respect their safety, agency, and confidentiality.

- **Localised:** Actions should apply global norms and frameworks to local contexts. Universal, rights-based standards should be upheld while adapting approaches to local realities, guided by empowered local civil society expertise.

- **Multi-stakeholder:** Actions must be taken in partnership across government, industry, and civil society to deliver meaningful change. Efforts should coordinate across sectors, avoiding siloes that fragment effective responses.

- **Life Course Approach:** Actions must recognise that risks, needs, and appropriate responses to TFGBV evolve across childhood, adolescence, and adulthood. Policy and design decisions should be age-appropriate and include meaningful participation of children and adolescents.

PILLAR 01

MANDATE SAFETY BY DESIGN THROUGH A POSITIVE DUTY, NOT A VOLUNTARY COMMITMENT

'Safety by Design' is a framework for the tech sector to proactively assess, mitigate, and engineer out harm, rather than solely responding after it has occurred. Tech that is safe by design not only prevents harm, but gives users control over their own experience and encourages pro-social behaviours. The core principles of Safety by Design are: service provider responsibility, user empowerment and autonomy, and transparency and accountability.[61] Safety by Design is increasingly recognised as a best practice in the tech sector, but industry-wide adoption and implementation lag. Mandating Safety by Design creates a baseline expectation that risk assessment and mitigation are fundamental to all tech design, delivery, and maintenance decisions. With proper resourcing and compliance and enforcement powers, this puts guardrails in place to stop companies from prioritising profits over safety.

For example:

- As the developer of the Safety by Design framework, Australia's eSafety Commissioner has issued implementation guidance and resources for tech companies, including industry guides focused on TFGBV and online child sexual exploitation and abuse. Under the Online Safety Act 2021, Australia is currently moving to legislate a "Digital Duty of Care" for all online service providers, which will embed Safety by Design principles and require due diligence from service providers.

- The UK's Online Safety Act explicitly requires regulated services to be "safe by design." Ofcom, the UK's communications services regulator, enforces Safety by Design requirements, including by requesting and reviewing annual assessments from user-to-user service platforms of the risk that UK users will encounter illegal content.[62]

Prevention Actions

CLOSE THE LEGAL GAPS ON TFGBV

There are stark gaps in how national legal frameworks address TFGBV. Drawing on global norms and frameworks, governments should ensure that existing laws, policies, and legal frameworks for GBV and cybercrime explicitly include TFGBV and provide clear civil and criminal liability. Definitions of TFGBV should be consent-based, rather than intent-based, and allow for contextual definitions of what is intimate and harmful. Legislation and policies should be regularly reviewed to ensure that laws and regulations are keeping pace with rapidly evolving technology and forms of TFGBV.

It is important to recognise that some State actors may misuse legislation and protections against TFGBV to surveil, silence, and abuse women, girls, and gender-diverse persons including human rights defenders and those in public life. Regulations and legislation must always meaningfully include survivor inputs and uphold human rights.

For example:

- Recognising the need to update and strengthen legislation on TFGBV, harmonise definitions, and reduce fragmentation across jurisdictions, multilateral and civil society organisations have produced model laws for governments to adopt. These include: Model National Framework for Addressing NCII, Model framework for legislation on technology-facilitated violence against women and girls, and the Inter-American Model Law to Prevent, Punish, and Eradicate Gender-Based Violence against Women.

- Mexico reformed its Criminal Code and Law on Women's Access to a Violence-Free Life, a suite of legislation known as "Ley Olimpia" named after a survivor advocate. These legal updates recognise, define, and include digital violence against women and girls, and punish "crimes against sexual intimacy," including image-based abuse, with fines and four to six years in prison.[63] Ley Olimpia has inspired similar legislative action across Latin America and the Caribbean.

PILLAR 01

Legal reforms adopted by governments[64]	Examples
Integration of TFGBV into new or existing GBV laws	In 2024, Chile adopted a Comprehensive Law against Violence against Women that explicitly recognises digital violence against women and girls as a form of GBV.
Integration of TFGBV into broader existing laws	In 2024, France strengthened its Penal Code to address emerging forms of TFGBV including the creation of offences relating to sexually explicit deepfake content and digitally manipulated intimate images.
Adoption of online safety or cybercrime laws that, among other issues, also cover TFGBV	In 2022, Botswana adopted the Cyber Crime and Computer Related Crimes Act, which addresses online harms including the non-consensual sharing of intimate images.
Adoption of specific laws that address one or some forms of TFGBV	In 2023, the Republic of Korea adopted the Act on Prevention of Stalking and Protection of Victims, criminalising deep fake sexual offences, online stalking, and other forms of technology-facilitated sexual exploitation. In 2025, the United States adopted the TAKE IT DOWN ACT, which criminalises the sharing or threat of sharing NCII and requires tech platforms to remove NCII within 48 hours of a survivor's verified request.

Prevention Actions

EMBED DIGITAL LITERACY, INCLUSION, AND NORMS CHANGE INTO NATIONAL PROGRAMS

Proactive prevention of TFGBV must include holistic, multi-sectoral programs, policies and investments that change the practices, structures, and norms that produce gender inequality and underpin the causes of all forms of GBV. Governments should integrate digital literacy, GBV prevention skills-building, and norms change into education and community-based programs targeting youth, parents, educators, and community leaders to help them understand the risks and benefits of technology, digital rights and hygiene, and available support services.

For example:

- 'Clic Derechos' is a nationwide program in Argentina that incorporates digital rights and online safety into school curricula and community initiatives. Led by the National Secretariat for Children, Adolescents and Family, it seeks to normalise conversations about TFGBV while strengthening young people's digital literacy.[65]

- In Indonesia, the Ministry of Communication and Information Technology launched a digital literacy program to educate the public on identifying and responding to technology-facilitated violence.[66]

- In Vanuatu, the government and multilateral partners developed a national Prevention Strategy on Online Child Abuse and Sexual Exploitation, reaching thousands of students, parents, and educators, resulting in improved online safety knowledge.[67]

PILLAR 02

REQUIRE ACCESSIBLE, TRAUMA-INFORMED REPORTING MECHANISMS FOR TFGBV

Governments should mandate that tech platforms establish clear and accessible reporting systems for survivors to report incidents of TFGBV. Reporting systems must be robust enough to meet demand and should be survivor-centred and trauma-informed, taking care not to retraumatise survivors and reducing the number of times they must relive their abuse. Laws and regulations should include clear timelines for the take-down of illegal content once tech companies are notified. Because TFGBV content is often shared and re-shared across multiple platforms, governments should also require tech company participation in cross-platform signal-sharing and collaboration on content removal.

For example:

- In Singapore, the Code of Practice for Online Safety requires designated social media platforms to proactively detect and take down egregious content and to provide user-friendly reporting mechanisms. This is complemented by the newly formed Online Safety Commission, which supports TFGBV survivors in the timely removal of harmful online content with an initial focus on intimate image abuse, image-based child abuse, doxxing, online harassment, and online stalking.

- In the UK, Ofcom now recommends that certain service providers use 'hash matching' technology to detect intimate image abuse and encourages providers to use a hash database such as StopNCII.org. Hash matching converts reported images into a unique string of numbers that can then be shared and matched against hash lists without ever seeing the image's content. This allows companies to detect image-based abuse across platforms and reduce its prevalence, while reducing revictimisation of survivors.

- In The Gambia, the National Child and Vulnerable Groups Online Protection Policy (2024) includes cross-government commitments to develop codes of conduct, protocols, and guidelines for internet service providers that will require reporting of and blocking access to illegal and harmful content.[68]

Response and Healing Actions

ENSURE NATIONAL RESPONSE SYSTEMS INTEGRATE TFGBV SURVIVORS

Too often, TFGBV survivors are separated from existing GBV reporting and response systems and have nowhere to turn for help and support. Governments must integrate TFGBV into existing multisectoral reporting and response systems (e.g. help-lines, support services through health systems, child and family support services), and build the capacity of frontline GBV organisations to address TFGBV alongside other forms of GBV, particularly as survivors may be experiencing multiple forms of violence simultaneously. Robust referral systems and pathways should be established to refer survivors to specialised services where needed. In developing national response systems and policies, governments must meaningfully integrate the needs and perspectives of survivors, such as by establishing National Survivor Councils.[69]

For example:

- In 2024, the National Center Against Violence in Mongolia delivered capacity-building training for shelter professionals to strengthen their ability to identify and respond to TFGBV, provide survivor-centred services grounded in human rights principles, and improve digital literacy and cybersecurity skills.[70]
- In Austria, the 24-hour women's emergency hotline in Vienna works with IT security experts and the Association of Vienna's Women's Shelters to provide a comprehensive response to specific cases of cyberviolence.[71]
- Resources for building the capacity of frontline providers to support TFGBV survivors include a tech safety checklist and a multi-sectoral training package for social services, health, policing, justice, educators, and the tech sector, developed by UNFPA. The training package is being adapted and rolled out regionally, including in Egypt.[72]

PILLAR 03

HOLD TECH COMPANIES TO ACCOUNT

Governments must implement accountability through strong compliance and swift enforcement, fines, and regulatory sanctions when laws and regulations are breached. This requires ensuring that regulatory bodies are adequately resourced and have the necessary authority and expertise to address TFGBV. Comprehensive laws and regulations will not be taken seriously by the tech sector without robust enforcement to back them. Compliance should include requirements for data transparency and public reporting to make accountability tangible.

For example:

- Following reports that xAI's Grok Imagine tool could generate sexualised deepfake content, regulators and courts in multiple jurisdictions initiated responses, including a Dutch court injunction requiring xAI and X to stop generating illegal sexual imagery, backed by daily fines for non-compliance.[73] The UK's Ofcom opened an investigation under the Online Safety Act,[74] while the European Commission initiated proceedings against X under the Digital Services Act.[75]

- In the United States, the Federal Trade Commission is requiring Pornhub's operator, Aylo, to establish a program to prevent the distribution of CSAM and nonconsensual material and pay a US$5 million penalty to the state of Utah. This enforcement action comes after Aylo allowed the dissemination of this harmful content, failed to review content flagged by users, and did not prevent the reupload of identified CSAM.[76]

- Three widely used AI-powered "nudifying" services have withdrawn from Australia after the eSafety Commissioner took enforcement action.[77]

Accountability and Justice Actions

STRENGTHEN THE JUSTICE SYSTEM TO DELIVER FOR SURVIVORS

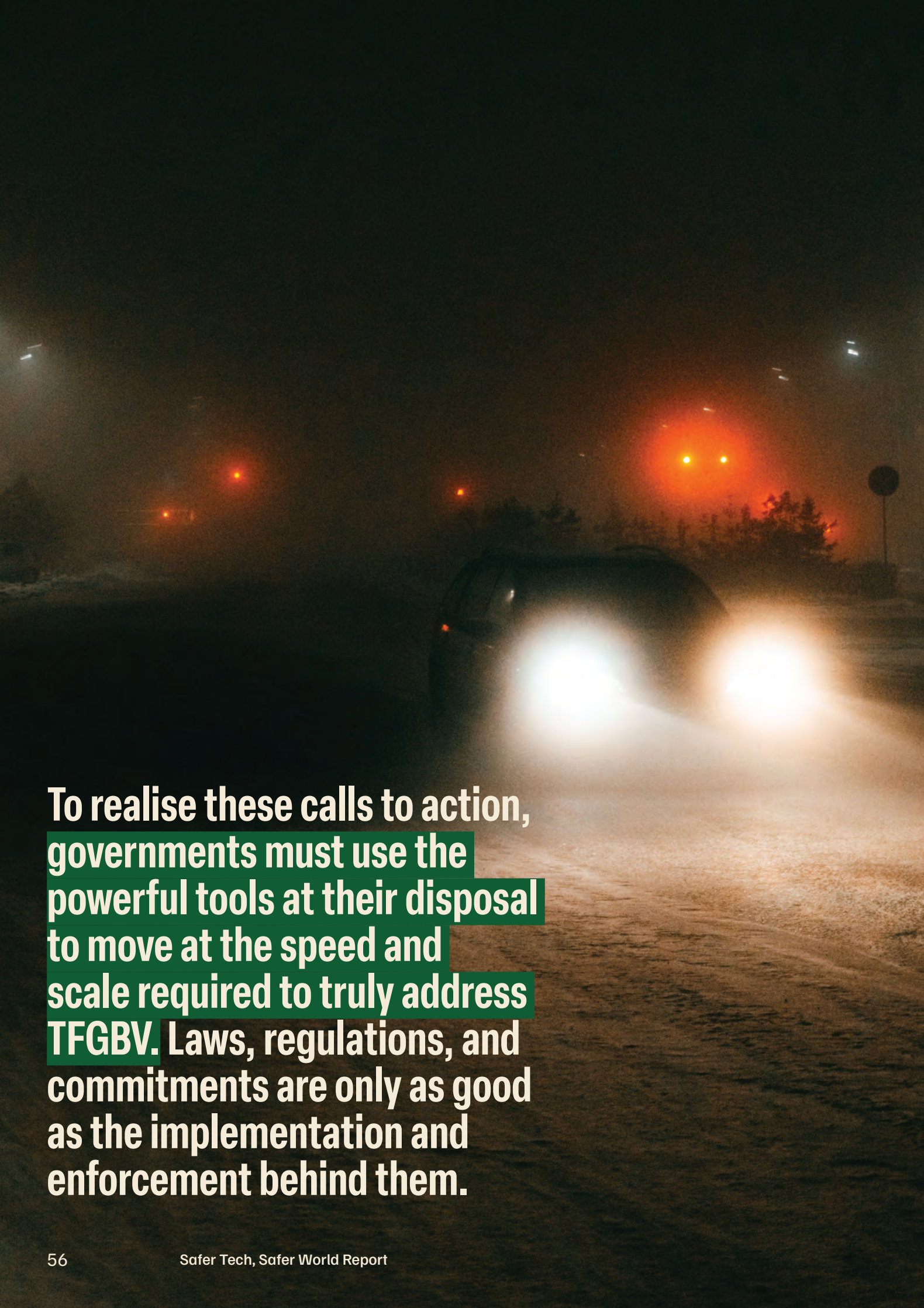
When survivors choose to pursue formal justice responses to TFGBV, they are too often left with insufficient responses or turned away. Police, judges, and prosecutors often lack an understanding of TFGBV and its impacts, and may be unaware of legal bases for intervention. Online harms like TFGBV require specific skills and considerations such as digital evidence collection and working with tech platforms on content removal. Governments must invest in building the capacity of justice system actors to better respond to TFGBV survivors in comprehensive, trauma-informed ways that respect survivors, ensure justice, and lead to accountability for perpetrators.

For example:

- The Pacific Islands Chiefs of Police established Cyber Safety Pasifika Programme, a regional approach to cybercrime prevention and response. The program builds law enforcement capacity using a 'by the Pacific, for the Pacific' approach to address online harms, including TFGBV, through training, awareness-raising, and locally led solutions.

- In Ecuador, the Ministry of the Interior created a National Specialized Unit for Cybercrime Investigation, which is trained on the collection of digital evidence, data analysis, and cooperation with service providers to respond to online harms like TFGBV.[78]

- There are growing resources on strengthening justice responses for TFGBV, including UN Women's specialised guidance for police and guidance from UNFPA and UNODC on adopting trauma-informed and responsive frameworks for policing and the justice sector.



To realise these calls to action, governments must use the powerful tools at their disposal to move at the speed and scale required to truly address TFGBV. Laws, regulations, and commitments are only as good as the implementation and enforcement behind them.

ENABLERS *of* CHANGE

- **Resourcing:** Governments must put money behind their commitments by including TFGBV prevention and response in national budgets. This includes ensuring laws and regulations are funded and have the staffing and authority for enforcement. Governments should prioritise TFGBV as part of development, democracy, and peace and security investments.

- **Movement Building:** Survivor-led, feminist movements have driven legal and policy change to prevent GBV and progress on addressing TFGBV to date. At a time when women's rights organisations face considerable backlash and funding cuts, it's more important than ever for governments to support and invest in them through core, flexible, and sustainable funding. This includes involving those with lived experience in policy design – government leaders can use their convening power to open direct lines between policymakers, survivors, and executives making product and policy decisions. Governments at all levels also have a critical role in supporting and funding evidence-based prevention initiatives that engage and mobilise men and boys as allies and partners in this vital work.

- **Global Governance and Collaboration:** A borderless problem requires a collaborative, borderless response across governments. Global and regional human rights bodies, coordination bodies, partnerships, and governance frameworks are essential to harmonise approaches, inspire national action, expand influence with the tech sector, and create accountability across jurisdictions. Digital governance frameworks, such as the Global Dialogue on AI Governance, are key opportunities for government leadership to embed gender equality, survivor-centred approaches, and real accountability.

- **Evidence Generation:** Data and evidence gaps remain that limit our understanding of TFGBV and our ability to respond to it effectively, including around survivors from underrepresented communities, perpetration, nationally representative data in the Global South, conflict settings, and interventions from low-resource contexts. As legislation is adopted and solutions are rolled out, research is needed to better understand what works to address TFGBV and what Safety by Design approaches are most effective. Governments must support continuous data and evidence generation so the true, evolving scale and nature of TFGBV can be measured, funded, and addressed.

All In is calling on government leaders and decision-makers to take courageous, collective action to address TFGBV through a duty of care. In line with All In's approach articulated in our founding Position Paper, we are advocating for and supporting the implementation of this report's recommendations by:

- Mobilising government leaders and decision-makers, including parliamentarians, at key global, regional, and national convenings and through individual and collective advocacy.
- Amplifying the voice and work of the GBV and digital rights ecosystems to share best practices and ensure that actions taken by governments and the tech sector draw on their expertise and learnings.
- Engaging new sectors, leaders, and partners outside of the GBV and digital rights sectors to address TFGBV, including through the next phase of our work which will focus on tech sector leaders, investors, and shareholders.

OUR COMMITMENT

ALL IN

GLOBAL LEADERS *for* ENDING GENDER-BASED VIOLENCE



ACKNOWLEDGMENTS

This report was written by the All In Secretariat (Equality Institute), based on inputs from All In Leaders, Expert Advisory Group, and Technology & GBV Working Group. We thank the following for their time, insights, and expertise.

Report Author: Caroline Cooney

All In Secretariat: Dr. Emma Fulu, Somali Cerise, Caroline Cooney, Sarah Vincenzini, Rebecca Ladbury

All In Leaders: Tarana Burke (Co-Chair), Maria Fernanda Espinosa (Co-Chair), Prof. Charlotte Bunch, Dr. Denis Mukwege, H.E. Ellen Johnson Sirleaf, Gabriela Ramos, H.E. Graça Machel, Geeta Rao Gupta, Baroness Harriet Harman, Julie Inman Grant, Mabel van Oranje, Ross Taylor, Dr. Sima Samar, Dr. Trang Nguyen, Victor Madrigal-Borloz, Vivir Quintana

All In Expert Advisory Group: Anna Nikoghosyan, Ben Hurst, Bettina Baldeschi, Daniela Ligiero, Diana J. Arango, Elizabeth Dartnall, Erin Kenny, Fatou Baldeh, Gary Barker, Hera Hussain, Jackson Katz, Joy Anderson, Kalliopi Mingeirou, Laxman Belbase, Lori Heise, Manisha Mehta, Marcus Daniell, Marwa Sharafeldin, Mary Ellsberg, Mona Sinha, Shanaaz Mathews, Sohini Bhattacharya, Tesmerelna Atsbeha

All In Technology & Gender-Based Violence Working Group: Alexandra de Filippo, Alexandra Robinson, Ayesha Mago, Barsha Chakraborty, Daniela Ligiero, Elizabeth Dartnall, Felicity Mulford, Hera Hussain, Laxman Belbase, Lori Heise, Kalliopi Mingeirou, Rachel Grant, Yasmin Chilmeran, Yeliz Osman



ENDNOTES

[1] Stevenson, J.G., Krzeczkowska, A., Moore, C., McFeeters, A., Li, S., Martellozzo, E., & Fry, D. (2026). Into the Light Index: Data update on global technology-facilitated child sexual exploitation and abuse 2026. Childlight, Global Child Safety Institute

[2] World Health Organization Regional Office for Europe. (2025). Addressing the digital determinants of young people's mental health and well-being: Policy brief. Web annex: Findings from evidence review and policy mapping. WHO Regional Office for Europe.

[3] Hayes, C., Gupta, T., Crockett, C., & Bansal, V. (2026). Engaging men, ending violence: Pathways to safer digital futures. UN Women and Equimundo.

[4] Craanen, A., & Tarrant, F. (2026). Addressing the intersection of misogyny, targeted hate and violent extremism. Institute for Strategic Dialogue.

[5] Dunn, S., Vaillancourt, T., & Brittain, H. (2023). Supporting safer digital spaces. Centre for International Governance Innovation.

[6] UN Women. Forthcoming rapid review on TFVAWG.

[7] Dunn, S., Vaillancourt, T., & Brittain, H. (2023). Supporting safer digital spaces: Special report. Centre for International Governance Innovation.

[8] UNFPA. (2021). Technology-facilitated gender-based violence: Making all spaces safe.

[9] Plan International. (2023). Free to be online? Girls' and young women's experiences of online harassment.

[10] Dunn, S., Vaillancourt, T., & Brittain, H. (2023). Supporting safer digital spaces. Centre for International Governance Innovation.

[11] Harris, B., & Woodlock, D. (2021). "For my safety": Experiences of technology-facilitated abuse among women with intellectual disability or cognitive disability. Australia eSafety Commissioner.

[12] Glitch, UK. (2023). The digital misogynoir report: Ending the dehumanising of Black women on social media.

[13] Posetti, J., Hellmueller, L., Williams, K., Renaud, P., Aboulez, N., & Shabbir, N. (2025). Tipping point: The chilling escalation of online violence against women in the public sphere. UN Women.

[14] UNFPA. (2021). Technology-facilitated gender-based violence: Making all spaces safe.

[15] McGlynn, C., McDermott, Y., Macdonald, S., Toparlak, R., Tarrant, F., & Treacy, S. (2026). Invisible no more: How AI chatbots are reshaping violence against women and girls. Durham University, Swansea University & UK Research and Innovation.

[16] Woodlock, D. (2017). 'The Abuse of Technology in Domestic Violence and Stalking.' Violence against Women, 25 (5): 584-602.

[17] Amnesty International. (2024). Yemen: "my life was completely destroyed": technology- facilitated gender-based violence in Yemen.

[18] Posetti, J., Hellmueller, L., Williams, K., Renaud, P., Aboulez, N., & Shabbir, N. (2025). Tipping point: The chilling escalation of online violence against women in the public sphere. UN Women.

[19] UNFPA. (2021). Technology-facilitated gender-based violence: Making all spaces safe.

[20] Centre for the Study of Organised Hate. (2026). How algorithmic design of tech platforms normalizes gendered violence.

[21] Security Hero. (2023). 2023 State of deepfakes: Realities, threats, and impact.

[22] Chayn. (2026). Explicit harms of non-explicit images: Defining image-based abuse in Pakistan and the diaspora.

[23] Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S., & Kaufmann, Z. (2021). Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online. Wilson Center.

[24] UK Foreign, Commonwealth & Development Office. (2024). Global Partnership for Action on Gender-Based Online Harassment and Abuse calls for urgent action on countering gendered disinformation.

[25] Internet Governance Forum. (2021). Best practice forum on gender and digital rights: Exploring the concept of gendered disinformation.

[26] Posetti, J., Williams, K., Hellmueller, L., Renaud, P., Shabbir, N., & Aboulez, N. (2026). Tipping point: Online violence impacts, manifestations and redress in the AI age. UN Women.

[27] Plan International. (2021). The truth gap: How misinformation and disinformation online affect the lives, learning and leadership of girls and young women.

[28] Thorn & National Center for Missing & Exploited Children (NCMEC). (2024). Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data.

[29] Internet Watch Foundation. (2026). Harm without limits: How AI is being abused to create child sexual abuse imagery

[30] Plan International. (2023). Free to be online? Girls' and young women's experiences of online harassment.

[31] Economist Impact & Together for Girls. (2026). Out of the Shadows Index: Indicator 4.4 laws against online child sexual violence.

[32] Plan International. (2023). Free to be online? Girls' and young women's experiences of online harassment.

[33] Posetti, J., Williams, K., Hellmueller, L., Renaud, P., Shabbir, N., & Aboulez, N. (2026). Tipping point: Online violence impacts, manifestations and redress in the AI age. UN Women

[34] Womankind Worldwide. (2026). Unsafe by design: A tech-facilitated gender-based violence analysis.

[35] Lomba, N., Navarra, C. & Fernandes M. (2021). Combating gender-based violence: Cyber violence European added value assessment. European Parliamentary Research Service March 2021.

[36] Koch, L., Ghawi, R., Pfeffer, J., & Steinert, J. I. (2026). Online misogyny against female candidates in the 2022 Brazilian elections: A threat to women's political representation? Information, Communication & Society, 29(7), 2104–2124.

[37] ChristChurch Call Foundation. (2026). Catalyst: Addressing misogynistic pathways to violent extremism: Factsheet.

[38] UN Interregional Crime and Justice Research Institute. (2026). The digital frontline: Emerging evidence on technology-facilitated gender-based violence in fragile and conflict settings.

[39] Krivkovich, A., Goldstein, D., & McConnel, M. (2025). Women in the workplace 2025. McKinsey and LeanIn. Org.

[40] World Economic Forum. (2023). Global gender gap report 2023: Insight report.

[41] UNESCO, IRCAI. (2024). Challenging systematic prejudices: An investigation into gender bias in large language models.

[42] Semenzin, S., Kerby, N., Schuler, M., & Romano, S. (2026). Harassment as infrastructure: How Telegram's design enables technology-facilitated gender-based violence in Italy and Spain. AI Forensics.

[43] Hayes, C., Gupta, T., Crockett, C., & Bansal, V. (2026). Engaging men, ending violence: Pathways to safer digital futures. UN Women and Equimundo.

[44] Reset Tech & Equimundo. (2026). The grift economy: How young men are being sold fake belonging and fake wealth online.

[45] Fisher, K., Rice, S., & Seidler, Z. (2025). Young men's health in a digital world. Movember Institute of Men's Health.

[46] Affoum, N., Revacarren, I., Vohara, N., & Wodon, Q. (2023). Protecting women and girls from cyber harassment: A global assessment of existing laws. World Bank.

[47] Top 10 Takeaways. (2026). Global index on Responsible AI.

[48] Equality Now. (2021). Ending online sexual exploitation and abuse of women and girls: A call for international standards. Equality Now, Trust Law, & Thomson Reuters Foundation.

[49] Sexual Violence Research Initiative, UN Women, The Global Partnership, & APC. (2024). Technology-facilitated gender-based violence: Developing a shared research agenda. Sexual Violence Research Initiative.

[50] Jóźwiak, M., & Ohnesorge, J. (2026). Platform governance and technology-facilitated gender-based violence: Positioning the DSA in the EU's legal framework. DSA Observatory.

[51] AI Act: EP approves simplification measures and "nudifier" app ban. (2026). European Parliament.

[52] Adapted from: UN Women. (2025). Normative advances on technology-facilitated violence against women and girls.

[53] Safety Showcase: Reimagine Gender in Tech. (2025).

[54] Ipsos. (2025). Ipsos AI monitor 2025: A 30-country Ipsos global advisor survey.

[55] Kennedy, B., Yam, E., Kikuchi, E., Pula, I., & Fuentes, J. (2025). How Americans view AI and its impact on people and society. Pew Research Center.

[56] Sippy, T., Enock, F. E., Bright, J., & Margetts, H. Z. (2024). Behind the deepfake: 8% create; 90% concerned. Surveying public exposure to and perceptions of deepfakes in the UK. The Alan Turing Institute.

[57] Allyn, B. (2026). Jury finds Meta and Google negligent in social media harms trial. NPR.

[58] Vigers, B. & Lall, J. (2025). Americans prioritize AI safety and data security. Gallup.

[59] Poushter, J., Fagan, M., & Corichi, M. (2025). How people around the world view AI. Pew Research Center.

[60] UN Office of the High Commissioner for Human Rights. (2011). Guiding principles on business and human rights: Implementing the United Nations "protect, respect, and remedy" framework.

[61] eSafety Commissioner. (2026). Safety by Design.

[62] OfCom. (2026). Pressing platforms to prioritise safety by design: Scrutinising Year 2 risk assessments.

[63] Tornel, J.C. (2020). Government of Mexico Publishes Digital Violence Act. Global Compliance News.

[64] Approaches from: UN Women. (2025). Tracking countries' efforts on technology-facilitated violence against women and girls: Ending violence against women and girls.

[65] Sexual Violence Research Initiative & UN Women. (2025). Global trends to prevent and respond to technology-facilitated violence against women and girls: A compendium of emerging practices.

[66] Government of Indonesia. National report: Beijing Platform for Action +30: Indonesia. (2024). UN Women

[67] Spotlight Initiative. (2024). Vanuatu: Final narrative programme report (01 January 2020 – 21 December 2023).

[68] The Gambia's National Child and Vulnerable Groups Online Protection Policy. (2024).

[69] Rivera, R. & Haff, N. (2024). From silence to leadership: how national survivor councils can drive prevention, healing and justice. Brave Movement.

[70] Government of Mongolia. Comprehensive national-level report on the implementation of the Beijing Declaration and Platform of Action (2019-2024). (2024). UN Women.

[71] Government of Austria. Beijing +30: Status of the implementation of the Beijing Declaration and Platform for Action: Austrian report. (2024). UN Women.

[72] UNFPA. (2025). UNFPA rolls out TFGBV training package in Arab States. UNFPA.

[73] R. Jahangir. (2026). Dutch Court Orders X, Grok to Stop AI-generated Sexual Abuse Content. Tech Policy Press.

[74] Ofcom. (2026). Ofcom launches investigation into X over Grok sexualised imagery.

[75] European Commission. (2026). Commission investigates Grok and X's recommender systems under the Digital Services Act.

[76] U.S. Federal Trade Commission. (2025). FTC takes action against operators of Pornhub and other pornographic sites for deceiving users about efforts to crack down on child sexual abuse material and nonconsensual sexual content.

[77] Australia eSafety Commissioner. (2026). Another three 'nudifying' services go dark in Australia as regulatory pressure mounts over child safety concerns. eSafety Commissioner.

[78] UN Women. (2024). Ecuador: National specialized unit for cybercrime investigation. UN Women: Women Count Data Hub.

The All In initiative is funded by the Ford Foundation, Wellspring Philanthropic Fund, Fondation CHANEL, Minderoo Foundation, and the UK Government's Foreign, Commonwealth and Development Office (FCDO). The views expressed in this report do not necessarily reflect the UK or Australian governments' official policies.











