

NAVIGATING MEGATRENDS: The ICPD Programme of Action for a Sustainable Future



A Safe Digital Future

Acknowledgements

Authors: Alexandra Robinson (UNFPA), Bridget Harris (Monash University)

Contributors: Marwa Azelmat (RNW Media), Christopher Wilson (My Data Global), Nora Piay Fernandez (UNFPA)

Reviewers: Chennai Chair (Mozilla Foundation), Suzie Dunn (Dalhousie University), Neema Iyer (Pollicy), Tierney McCue (UNFPA), Jan Moolman (Numun Fund), Afroz Johnson and Gerda Binder (UNICEF), Toby Shulruff (UNFPA), Elizabeth Wilkins (UNFPA), UNFPA ICPD30 Reference Group, UNFPA Regional Offices, UNFPA Executive Committee, UNFPA Innovation Unit

Coordination, Editorial, Design and Production

Senior Editors and Overall Technical Coordination: Priscilla Idele (UNFPA), Rachel Snow (Consultant)

Strategic Oversight: Julia Bunting, Julitta Onabanjo (UNFPA)

Editorial: Gretchen Luchsinger (Words for the World)

Communications, Advocacy and Web: Ana Maria Currea, Jacqueline Daldin, Etienne Leue, Angélique Reid (UNFPA)

Design: Upasana Young (GlowDesign)

Operations and Administrative Support: Sara Abranyos, Ashby Anglin, Elsa Dufay, Abbas Omar, Rayola Osanya (UNFPA)

Copyright © 2024 United Nations Population Fund, all rights reserved.
Reproduction is authorized provided the source is acknowledged.

How to cite this publication: United Nations Population Fund (2024).
Navigating Megatrends: The ICPD Programme of Action for a Sustainable Future
ICPD30 Think Piece: A Safe Digital Future

July 2024

Disclaimer: The named authors alone are responsible for the views expressed in this publication.

Cover photo © UNFPA

Contents

1	Introduction.	4
2	Digital Technology for Development: The Dichotomy Between Innovation and Harm	5
	▶ Changing demographics.	9
	▶ Young people	9
	▶ Older persons	10
	▶ Economic opportunities	10
	▶ Universal health coverage	11
	▶ Migration and displacement	13
	▶ The climate crisis	13
	▶ Movement-building	14
3	Realizing Digital Dividends	15
	▶ Design of technology	15
	▶ Deployment of technology: digital inclusion	19
	▶ Factors affecting access and use of technologies	21
	▶ Business models of technology	23
4	Recommended Actions	28
	▶ Digital inclusion	30
	▶ Safety-by-design.	30
	▶ Business models of technology	31
	▶ Regulation	32
	▶ Prevention	32
5	Conclusion	33
	References	35
	Endnotes	44

In a rapidly evolving digital world, the principles and commitments of the Programme of Action remain universal and valid

In mid-2024, UNFPA issued five think pieces to mark the thirtieth anniversary of the landmark 1994 International Conference on Population and Development (ICPD). Under the framing of *Navigating Megatrends: The ICPD Programme of Action for a Sustainable Future*, the five think pieces are titled:

- ▶ Demographic Change and Sustainability
- ▶ The Future of Sexual and Reproductive Health and Rights
- ▶ The Future of Population Data
- ▶ ICPD and Climate Action
- ▶ **A Safe Digital Future**

The think pieces explore ways to sustain, refresh and accelerate ICPD commitments in a world of radical transformation designed for policymakers, they reflect on progress and highlight likely future scenarios. They offer starting points for discussion on what's next for population, development, and sexual and reproductive health and rights (SRHR).

This think piece highlights key findings and recommended actions on how digitalization can support the future-proofing of the ICPD

This think piece provides recommendations for future-proofing the ICPD Programme of Action in the face of rapidly emerging digital technologies that serve to both advance and hinder progress.

Digitalization has enabled rapid economic growth and development in the last 30 years. Often underpinned by profit-driven business models, however, the design and deployment of digital technologies may amplify existing inequalities with unique risks for women and girls in all their diversity.

In a world increasingly characterized by digitalization and the rapid proliferation of technological innovation, the urgency to protect and advance progress towards realizing the ICPD Programme of Action cannot be understated. Safeguarding measures, innovative alternative business models, and effective and cross-jurisdictional regulation to protect, promote and respect human rights, including the principles of the ICPD, throughout the design and deployment of technologies must take place to future-proof the Programme of Action.

1 | Introduction

Since 1994, the world has been experiencing a digital transformation that offers great potential to accelerate and revolutionize progress towards the fulfilment of the ICPD Programme of Action. For these technologies to advance progress, however, it is critical to account for the ways in which digital technology can both enhance development agendas and pose potential risks

and harms. If technological advances continue to rapidly evolve without rights-based approaches to inclusion, privacy and safety, they may undermine the vision, values and principles of the Programme of Action.

By examining the **design, deployment** and **business models** of digital technologies, this think piece maps evidence-based recommendations for mitigating harms and increasing benefits through safety-by-design, digital inclusion and governance, capitalizing on digital technology to fulfil and “future-proof” the Programme of Action. Future-proofing is about being able to understand and continually evolve solutions and approaches in anticipation of the future. To ensure that progress on the Programme of Action continues, we must future-proof it against the harms associated with a digital world.

The think piece is divided into three parts. The first section outlines the dichotomy between innovation and harm in digital technologies that can support development outcomes (Box 1). A second section unpacks the design, deployment and business models of technology to adequately support evidence-based interventions and regulation to reap digital dividends. The final section draws together the breadth of evidence to identify inclusive recommendations to future-proof the Programme of Action.

BOX 1

A definition of digital technology

“Digital technology” or simply “technology” in this think piece encompasses the breadth of information and communication technologies (ICTs) that form digital public infrastructure.¹ These terms include but are not limited to telecommunication devices (landline telephones, mobile phones, tablets, computers and the like), location information, digital images, assistive devices, data, artificial intelligence (AI) and the Internet of Things (physical and digital systems connected via the Internet and other networks). The terms also include emerging technologies at the forefront of development and innovation.

2 | Digital Technology for Development: The Dichotomy Between Innovation and Harm

Digital technologies have accelerated globalization, transformed education and labour markets, and shifted lifestyles, health management, social interactions and civic engagement.² They expand opportunities for people in all their diversity to share and gather knowledge, access education and economic opportunities, engage in democratic discussion, build community, power movements and resistance, exercise their rights, and share their voices and interests.³ Digital access to information, services and resources increases capacity and skill sets, and fosters empowerment and agency. Safe and ethical technology helps to respect, protect and promote the dignity and rights of all people, which sit at the heart of the Programme of Action and sustainable development.

Strengthening the opportunities and capabilities of all people is crucial for social and economic development. In this, it is critical to prioritize the needs of persons furthest behind, particularly those living in poverty or with disabilities, people of African descent or from Indigenous communities, LGBTQIA+ (lesbian, gay, bisexual, transgender, queer, intersex, alternatives plus) and the most marginalized women and girls.⁴ It is equally critical to recognize these populations as agents of change. Sustainable development is not possible without placing human rights, including the participation of the most marginalized, at the centre of all efforts. It is also imperative that these efforts account for the uneven impacts of global megatrends, including digital transformation, the climate crisis, migration and shifting global demographics – all topics covered in related think pieces in this series.

It is widely promised that digital transformation can accelerate sustainable development. Innovation in technology systems in areas as diverse as communications, data, security, agriculture, biomedicine, transportation, energy and civic life is driven by, and dependent on, infrastructure that is global in scale. While some of these technologies are beyond the scope of this paper, they have effects on women and girls in all their diversity at the individual, community and structural scales, shifting patterns of employment, migration, climate, health, education and well-being. They operate through the same energy and communications systems as digital technologies, which are the focus of this paper. Innovation and decision-making about all these systems are centred in higher-income countries, with the systems then deployed in low- and middle-income countries. This imbalance is mirrored in every country between political and financial centres and lower-income communities.

Technological systems are also social systems; social values and biases are deeply embedded in innovation from the start.⁵ New and emerging technology is built from existing technologies and depends on existing systems, carrying with it legacies of inequalities and the uneven distribution of benefits and harms. Further, when innovation is done in labs and design studios by a relatively narrow set of actors who lack the perspective and context of the most marginalized, it results in uneven impacts in terms of benefits and harms along the entire supply chain, from resource extraction to manufacturing, distribution, use and eventually disposal. As a result, products and services meet the needs of users who resemble the designers and the most profitable market of consumers. Systems are optimized according to the assumptions and priorities of dominant groups, which then serve to reproduce and amplify discrimination.⁶ For example, when digital public infrastructure makes services available at scale, this may deepen inequality as those who are most

marginalized (and who may be illiterate or without access to devices and connectivity) are excluded from access to basic services, including social services, identification cards and health services. The most marginalized may also experience a disproportionate share of risks and harms.

To future-proof sustainable development and the ICPD Programme of Action, a frame of reference for risks and harms associated with technological opportunities must be provided

To determine how to future-proof sustainable development and the ICPD Programme of Action, it is critical to provide a frame of reference for risks and harms associated with technological opportunities. This should consider impacts across the micro/individual, meso/community and macro/structural levels of society.⁷

- ▶ **Individual:** Technology-facilitated gender-based violence (TF GBV) impacts how individuals participate in, use and benefit from digital technologies (Box 2). A European study found that women are 27 times more likely to face harassment online than men. Generative AI tools are increasingly being used to create and distribute deep fake images and videos with speed and targeted strategies to maximize harm.⁹ AI tools used for screening CVs and resumes for employment may remove women of reproductive age from shortlisting processes, based on bias that reflects existing patriarchal systems. A lack of access to digital devices and connectivity can in turn restrict an individual's access to essential services and information, including legal identity and emergency services. The experience of intimate partner violence, encompassing femicide, is amplified by technology.¹⁰
- ▶ **Community:** Young women are increasingly using digital spaces to make their voices heard or influence global affairs and are therefore the most at risk of being dissuaded as active citizens who raise awareness and advocate for important rights.¹¹ Fifty-one per cent of young women hesitate to engage in online debates after witnessing or directly experiencing online abuse; while 92 per cent of women report that online violence negatively influences their well-being.¹² The removal of women's and youth voices from community discussion impacts mechanisms of accountability as well as peer-to-peer support. Surveillance and location-tracking devices and data relating to access to SRHR clinics may place women and girls seeking services at risk of harm or even shut down services altogether. Technologies can hinder movement, allowing States, smugglers and traffickers to track and locate migrants, making people vulnerable to detection, arrest and abduction. Automated decision-making technology, including facial recognition software deployed at borders and in asylum and visa application reviews, may increase the rate of false positives due to inadequately diverse data sets. This can further marginalize already excluded communities, resulting in discrimination and unjust deportation.¹³
- ▶ **Structural:** Structural harms may persist through sustained and targeted disinformation campaigns against women running for public office. A survey of politically active women in Kenya found that 20 per cent of those surveyed had paused their social media activity in response to online violence; 38 per cent of women journalists reported making themselves less visible in their workplace because of TF GBV.¹⁴ Engagement-driven and content-agnostic social media platforms promote the proliferation of violent and misogynistic content, intensifying and normalizing harmful social and gender norms. This same mechanism can fuel hate speech and racially and ethnically targeted violence. Internet shutdowns and restrictions may prevent communications, limit free political debate, prevent immediate access to critical

BOX 2

...[t]he ubiquity of the Internet means that TF GBV can become omnipresent and relentless, infiltrating a victim's most intimate physical spaces, such as their home or bedroom. Users engaging in TF GBV can also leverage their own and targeted individuals' online social networks to further the abuse, by recruiting others to knowingly or unwittingly share abusive material, and by contaminating the targeted individuals' own online spaces and communities. The online permanence of abusive material – which is exceedingly difficult to completely eradicate once shared online – also ensures continued revictimization, resulting in lasting psychological and other damage.⁸

life-saving services, permit the proliferation of harmful and misleading content, and make a major contribution to the deterioration of human rights.¹⁵ Cyberattacks on hospitals can effectively shut down diagnostic and data collection systems, potentially harming the health and well-being of all patients. The rapid adoption of digital technologies aimed at increasing the efficiency of health-care delivery has amplified inequalities in access to health-care resources in some contexts as levels of meaningful connectivity are uneven. Infodemics – the rapid spread of an excessive amount of information, including false or misleading information – in health services have spurred confusion and mistrust among health authorities and led to the rejection of public health recommendations.¹⁶

In the context of key areas of the ICPD Programme of Action and global megatrends, this paper now highlights the dichotomy between technology as innovation and the associated risks and harms that should be addressed in order to ensure that we protect, respect and promote human rights and equalities.



© UNFPA

Changing demographics

Countries are demographically more diverse than ever before, with falling fertility rates and large-scale population ageing in some countries, and relatively high fertility and large youth populations in others.¹⁷ Technology provides avenues to support advanced understandings of population dynamics through digital and computational demography. New and emerging data sources from digital technologies, as well as these technologies themselves and improved computational methods, are advancing understanding of population dynamics. Faster and more precise data about population outcomes are being leveraged in relation to health, fertility and migration, for example, assisting evidence-based policy and programming.

Increasingly, microsimulation and agent-based modelling (individual-level simulations) provide digital tools that can function as virtual laboratories to test the impacts of policies relating to fertility, older adults, bereaved people and other social issues. Such tools provide insights into policy-relevant demographic changes shaped by megatrends such as ageing, climate change and migration. Digital tracing can facilitate real-time monitoring of populations, chart demographic change and guide interventions, including early warning systems for disaster prevention and recovery. It can also show the effect of social responses and policies.¹⁸ In short, the digitalization¹⁹ of population and development data and the possibilities these offer for scenario-building and projections of population dynamics can transform global, regional and national policies and strategies to promote and protect human rights.

Harms may be experienced across the frame of reference outlined above. At the individual (micro) level, the collection, access and release of information about fertility and sexual and reproductive health (SRH) can pose risks to women, particularly where contraceptive use or abortion are socially unacceptable or criminalized by the State. At the community level, this rich data set can be weaponized against marginalized groups based on ethnicity, gender or sexuality. At a structural level, inherent bias in data collected, which may only be representative of primary users who are predominantly men, may limit the accuracy of analysis and subsequent policies and programmes.

Young people

Technology can support burgeoning youth populations²⁰ with increased access to education and employment opportunities. This can advance women's and girl's economic status and security, and the economic growth of their communities.²¹ The digital revolution can overcome the "triple crisis" in education, which comprises: high rates of inequity and exclusion; a lack of foundational education in many settings; and outdated or irrelevant curricula that do not equip students with skills, knowledge and values to succeed.²² Technology can support quality education and transform progress in pedagogy, curricula and access, including through remote education. Digital technology can also enable shifts in power structures within communities and among countries, fostering academic freedom and addressing marginalization and discrimination through the decolonization and democratization of knowledge production and learning.²³

Increased access to quality SRHR information, services and supplies for adolescents and young people can change their lives and experiences. Greater uptake of digital technology can improve their awareness and use of health and social services, providing safe spaces to access knowledge and care that might otherwise be unavailable and inaccessible, or even false and misleading.

Adolescent girls, however, are a growing target group subjected to TF GBV by virtue of their rising engagement in and use of technologies and digital spaces.²⁴ For example, 80 per cent of images in cases of child sexual abuse materials are of girls aged 11 to 13 years.²⁵ Adolescent girls are more often subjected to sexual digital abuse within the context of dating violence.²⁶ As many as 58 per cent of adolescent girls and young women have been harassed online, according to a study by Plan International, and 85 per cent of those experienced multiple types of TF GBV, including abusive and insulting language (59 per cent), body shaming (39 per cent), threats of sexual (39 per cent) and physical violence (21 per cent), sexual harassment (37 per cent) or stalking (32 per cent).²⁸ Additionally, the use of social media platforms may have an important negative impact on the mental health of young people, particularly adolescent girls (Box 3).

BOX 3

Two thirds of American teenagers use TikTok, and the average viewer spends 80 minutes a day on the application. Within 2.6 minutes, TikTok recommended suicide content. Within 8 minutes, TikTok served content related to eating disorders. Every 39 seconds, TikTok recommended videos about body image and mental health to teens.²⁷

Older persons

For the growing proportion of older persons in the world, digital media and devices can offer dignity, autonomy and self-determination. Social isolation can be reduced and well-being facilitated by digital contact with family, friends and communities. Upskilling in digital and tech spaces as well as the availability of digital literacy training can increase the confidence of older adults, and provide opportunities for employment, socializing, health care, civic engagement and the management of finances. Technologies can also extend the health, well-being and independence of older people in later stages of life through smart sensor monitoring, assistive devices and robotics.

Given comparatively limited digital literacy among older adults, the risk of harm through, for example, scamming and phishing is significant. At a meso level, the lack of access to technology among older adults can prevent links to health-care or financial systems to maintain their well-being. Finally, data collected to design technologies, including AI, may become increasingly biased against older adults given their lower use of technology.

Economic opportunities

Technologies can provide more (and supplementary) employment, including for women and people with disabilities. Remote work, especially for women in rural communities, is more widespread, flexible and “family friendly” for women who are carers. ICTs and the Internet can help secure wider access to credit, resources and support to establish entrepreneurial ventures and businesses and develop careers.²⁹ Older women who face losses of jobs, safety nets and social support mechanisms can benefit from online businesses and economic opportunities. In countries where women’s access to education and employment are limited, online employment opportunities remain available, supporting economic independence and livelihoods.³⁰

Unequal access to meaningful connectivity, however, may mean that men’s employment options continue to increase while women’s opportunities remain stagnant, thereby increasing gender poverty margins. At an individual level, increased access to technology for women for employment

may result in targeted TF GBV. Technologies can also be harnessed for financial abuse, which can involve controlling access to accounts or purchases, or fraudulent transactions and loans.

Universal health coverage

At a normative level, universal health coverage must efficiently and equitably provide predictive, pre-emptive, personalized and participatory health care that enables people to live healthy, productive lives. People should be active participants in their own care: empowered to better determine their own health outcomes and able to understand, control, protect and leverage their own health information. This requires concrete progress on three fronts: providing all people with access to services; offering a full spectrum of essential, quality health services; and protecting people from overwhelming financial consequences from paying for health.

Digital technology offers enormous potential for expanding universal health coverage,³¹ enabling a more data-driven health sector to ensure evidence-based, targeted access to quality services by more efficient means. For example, the use of mobile or wireless technologies to deliver health-care services has increased uptake in remote areas and expanded the reach of new knowledge guiding diagnostics and treatment.³² Technologies can help overcome physical barriers (such as the distance to providers in rural or remote locations) or physical disabilities and/or social conditions that may limit people's movement. Clients can access services and support online, from their location, without having to travel. This is significant, as in non-urban areas, public transport networks, if available, are often fragmented, and private transport (such as taxis, hire cars or ridesharing) are expensive. Disability-accessible transport is sparse.³³




© UNFPA

Digital media and devices may also help to breach temporal barriers. Technologies may offer quicker access to health-care services than traditional in-person services, and result in greater productivity and efficiency. Additionally, while the resourcing of in-person health care and related services can limit the numbers of clients assisted and opening times, Internet pages, applications and AI-powered chatbots can provide “out-of-office” assistance and information at any time. There can be costs in establishing these technologies, but once they are running, required human and financial resources might be low or non-existent.

Technologies may also mitigate social barriers. In some communities, help-seeking and accessing health care, especially SRH care, may be stigmatized or taboo. Digital channels can provide private out-of-area services to alleviate some in-community risks and provide anonymity.³⁴ Including digital interventions in health systems can also raise awareness about sexuality, sex, contraception and childcare.³⁵ This is useful for survivors of GBV, given social barriers and stigmas around seeking treatment, support and help to escape violence. Since the COVID-19 pandemic, strategies and capabilities in digital and machine service provision have grown. Lessons learned from remote assistance continue to guide and extend access to geographically and socially isolated women and girls and those with disabilities.³⁶

The accuracy of prevention, screening, risk assessment, diagnosis and treatment tools is bolstered by technologies, enhancing the usability and quality of health-care experiences and outcomes for patients. AI applications in areas such as cancer treatment are revolutionizing patient care by enabling more personalized and precise approaches, leading to rapid drug development, higher recovery success rates and reduced side effects in cancer therapies.³⁷ Digital health technologies and machine learning applications can offer women and girls choice and agency in how they manage their SRHR. This might involve realizing intentions for childbearing and enabling access to contraception, services to address infertility, and antenatal, delivery and postnatal care to reduce high-risk pregnancies and the likelihood of maternal and newborn mortality. Services can target GBV, including in relation to sexual violence; intimate partner, domestic and family violence; and female genital mutilation.³⁸



**Technologies
have also aided
in the modelling,
prediction and
surveillance
of disease and
adverse events**

Technologies have also aided in the modelling, prediction and surveillance of disease and adverse events. This can slow and even prevent the spread of outbreaks, and inform responses and decisions, planning and the allocation of resources, and health systems management. Evidence and health-care research can be strengthened through data and intelligence, informing innovative responses.³⁹

Digital and machine learning health-care services could improve access and outcomes for all people, particularly women and girls. The provision of medical information or more accurate diagnosis does not necessarily translate into better, more appropriate, or equal access to treatment for women and girls. Similarly, digital education, campaigns and services related to GBV do not guarantee increased safety for survivors or the prevention and reduction of gender-based violence.

Migration and displacement

In a world characterized by increased movements of people as a result of economic conditions, the climate crisis and/or conflict, technologies can better map vulnerability and identify how to support populations who seek to migrate or are displaced. Location trackers (Global Positioning System, GPS) allow people to orient themselves on journeys, which can reduce reliance on smugglers and dangerous routes.

The majority of people who migrate do so for a range of push and pull factors. Migrants include refugees, who often arrive in places they know little or nothing about. Some rely on information from traffickers who smuggle them across borders. Even highly skilled newcomers can be rendered helpless by institutions, laws and practices that differ from those in their home country. Local bureaucracies may impose thorny requirements involving the securing and updating of certain documents. Language barriers can affect everything from obtaining food and lodging to navigating legal mazes. A range of supportive technologies includes, for example, Signpost and one of its tools, Refugee.info, which delivers reliable information in five languages and reaches 70 per cent of some 50,000 refugees in Greece.⁴⁰ Digital media and devices can provide people with information and a way to build networks and establish their lives in a new country.

Technologies can also present harmful human rights risks during migration. Traffickers may use migrants' phones or other devices to track and control their movements. The use of automated visa application systems and unrestricted use of algorithms can lead to harmful profiling, perpetuating discrimination. Drones and automated recognition tools used to detect movement on extended border areas have been reportedly used to stop migrants from arriving there. Where surveillance prioritizes control rather than life-saving assistance, more dangerous migration routes may emerge and borders may become sites of human rights violations instead of offering sanctuary, dignity and human rights protections to which people on the move are entitled.⁴¹

The climate crisis

Developing and transferring technologies to support national action on the climate crisis have been essential elements from the beginning of the United Nations Framework Convention on Climate Change process.⁴² A Technology Mechanism established under the Convention consists of two complementary bodies: the Technology Executive Committee and the Climate Technology Centre and Network (CTCN). The CTCN has established itself as a centre for climate technology support and information with a global network of more than 150 organizations that assist developing countries in finding climate technology solutions. Emerging technologies cover a broad range of both mitigation and adaptation issues and reflect the diverse challenges that different countries face. For instance, the CTCN helped Bhutan to reduce greenhouse gas emissions from public transport. It supported Namibia in developing a water harvesting plan. Other tech innovations include, for example, Google's Flood Hub alert system, which uses machine learning technology to warn people when rivers, oceans and lakes pose a threat to life or property. AI can be applied to improve hazard forecasting for regionalized long-term events, such as sea-level rise, and for immediate, extreme events such as hurricanes, among other possibilities. These applications include the management of vulnerability and exposure, such as by developing infrastructure that can minimize climate hazards.⁴³ The Internet of Things is being used in Brazil, Italy and Spain to manage and maximize water supplies for agricultural use.⁴⁴



The tech industry significantly contributes to the climate crisis through energy-intensive operations, including data centres, manufacturing processes and electronic waste generation. These harms disproportionately impact already vulnerable communities. Additionally, an overreliance on technology to address climate change may obfuscate the need for participatory approaches to mitigation and adaptation measures centred on the experiences of those most adversely affected, including, disproportionately, women and girls.

Movement-building

Central to the ICPD Programme of Action is a holistic and multisectoral approach to development, and therefore, partnerships across civil society, faith-based organizations and leaders, and youth and feminist movements. Technology has opened a world of new possibilities for the networking and mobilization of movements, including of marginalized groups, enabling them to organize, learn and express themselves despite societal surveillance. Online women-led and feminist campaigns have helped to boost the financial, social and cultural capital of women and girls in and beyond the home, and to improve their self-esteem, self-efficacy, inclusion, agency and empowerment.

The Internet and social media are key sites for political activism and resistance, networking and opportunities to create and maintain communication, communities, allies and relationships. Local movements can be networked into global movements through digital technologies.⁴⁵ Marginalized and oppressed voices can be broadcast to reach policymakers and practitioners. As civil society spaces shrink and backlash threatens women's rights movements,⁴⁶ technology has a central part in maintaining the priorities of the Programme of Action.

Online engagement in movement-building may, however, catapult women human rights defenders into the sights of harmful anti-women's rights movements, placing individual women at risk of harm. There are difficulties, too, in measuring and benchmarking the gains of various movements.

When they are successful, audience engagement, solidarity, collective humanizing, empathy and investment prompt action. Yet this will not happen if responses are superficial or performative, or depend on the lazy sharing or promotion of social media posts without any effort to pursue structural or systemic changes.

3 | Realizing Digital Dividends

Technology holds great potential to accelerate and advance the Programme of Action. Realizing this requires avoiding the romanticization of technology or the overstatement of its benefits. Considerable investment in rights-based technologies, safety, privacy, participatory design, accessibility, resourcing, capacity-building and meaningful connectivity is needed to realize digital dividends, improve quality of life and women's and girls' abilities to exercise their rights, and enhance opportunities for agency and freedoms.

In addressing harms and balancing human and technological innovation to drive forward progress, it is critical to address key aspects of technology related to **design, deployment** and **business models**.

The design phase refers to creating a technology and defining its functional and physical features. This process includes research, problem definition, ideation, prototyping and testing. Key interventions should be integrated throughout this process to mitigate harm and promote rights-based access and use. The deployment phase speaks to the process of uptake and use of the technology, when the heterogeneity of users impacts the ways in which they access and apply technology. Key barriers can arise that must be understood, addressed and overcome. Business models, guided by effective regulation and interventions, should be sustainable and protect the rights of users.

Across all three phases, the United Nations Guiding Principles on Business and Human Rights provide a fundamental framework for all companies, regardless of industry, size, structure or operating context. The Guiding Principles identify risks to people and steer actions to prevent or mitigate them. This process includes the expectation that technology companies make efforts to anticipate and mitigate harms that might occur from using their products and services.⁴⁷ This think piece provides an in-depth perspective on the design and deployment of technology within the context of business models, including through applying the Guiding Principles to protect, promote and respect human rights and to future-proof the Programme of Action.

Design of technology

For technology to accelerate and advance the Programme of Action, the potential for negative consequences in design, development, management and use must be prevented and mitigated. Technology, whether used for malicious or well-intentioned purposes, is often created without consideration for how it could deepen inequalities and cause individual and systemic harms. That is, regardless of whether technology is well-intentioned or otherwise, if it is poorly designed, it will carry some risk of harm (Box 4). Figure 1 depicts how harms experienced by users will be the same, regardless of intention or motivation, if technology is not rights-based and designed with safety, security and privacy at its heart.

BOX 4

An example of how better information access compromises privacy

An app designed to increase access to information about sexual health for young people may be designed to empower young people to understand their rights and choices. But poor design may permit the sale of user data to an actor who will use them to push out harmful anti-rights and choices information.

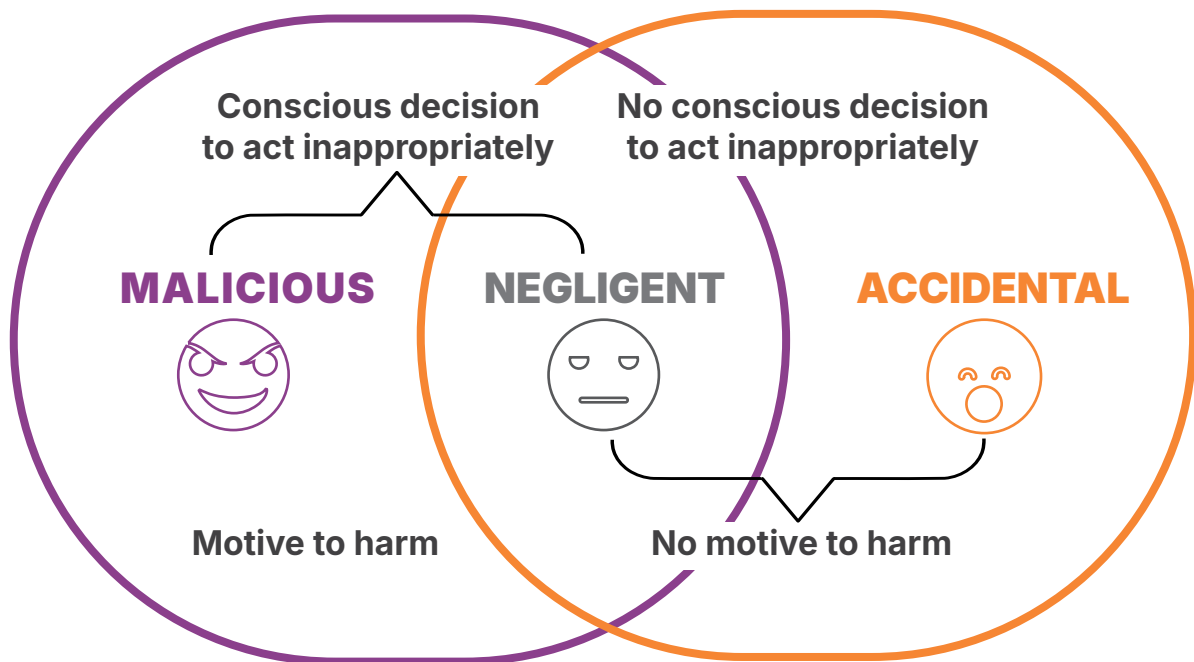
The human-rights based approach is underpinned by five key principles: participation, accountability, non-discrimination and equality, empowerment and legality. Design that considers all these principles will ensure protection, promotion and respect for human rights.

Technology has been largely built for idealized interactions of users, with often limited assessment of the potential for harm or for ways to enable the power and agency of the most vulnerable users.⁴⁸ Giving preference, whether intentional or otherwise, to the rights of dominant groups through the design and deployment of technology

can reproduce and amplify discrimination. This is exacerbated by a profit-driven industry that prioritizes financial returns over safety, promulgating a “move fast and break things” mentality. By contrast, rights-based interventions prioritize the rights and needs of users, applying the principle of “do no harm”. To redress the inherent tension between the two, safety-by-design approaches incorporating principles of privacy, security and safety (as well as rights-based approaches)

▶ FIGURE 1

Harms to users will be the same, regardless of intention, if risks are ignored in design



Source: UNFPA 2023, p. 9.

ought to be baked into proofs of concept as well as design, deployment and monitoring systems. Safety-by-design proactively embeds safety and risk mitigation strategies into the design and development of products and services. The focus is on minimizing risk by anticipating, detecting and eliminating harm before it occurs, rather than providing safeguarding measures after an issue arises.⁴⁹ Safety-by-design is a critical component of future-proofing the Programme of Action and harnessing the potential of technology.

Design pedagogies must be employed that centre on the voices of those directly impacted by design process outcomes; the impact on communities over designer intentions; and everyday people as experts on end-user⁵⁰ experiences who collaborate with designers and developers. This approach mandates the participation of women and marginalized populations in the financing/funding of tech development, and includes the ideation, conceptualization, development, testing and scaling of products that have accessible safety features and complaint mechanisms in their solutions and platforms. To understand user needs, safety issues and concerns, platforms and services should meaningfully engage with diverse women and girls, including marginalized groups. Platforms can consult and make user agreements with them.⁵¹ Governments and businesses must ensure women have active roles in internal staffing across all roles and levels of responsibility, including in decision-making.⁵²

Women and marginalized communities are a tremendous resource for ideation and conceptualization of tech products. They can also provide functional specifications to meet their needs as end-users.⁵³ Examples of design approaches include responsible innovation, human-centred design, value-sensitive design and design justice.⁵⁴ Even these approaches mirror technology development challenges as they originate in higher-income countries and therefore reproduce and amplify existing inequalities. Efforts are ongoing, however, to collaboratively define design and innovation processes that are contextual, local and equitable.⁵⁵ Threat modelling and gender-inclusive user testing are other critical processes for identifying design concerns in the end-user interface.⁵⁶ For example, location trackers help find lost objects but have also been used to illegally stalk women. This viewpoint may be missed if the perspectives of women, one in three of whom are estimated to be survivors of intimate partner violence at some point in their lives, are not central to ideation and design processes.⁵⁷

Including women, girls and those disproportionately impacted by TF GBV in user testing is essential. User testing questions must explicitly address gendered dimensions and potential applications of tech products that may enable, assist, aggravate or amplify GBV. The absence of measures such as "quick exit" options on websites, for example, can increase exposure to risks of violence, especially for marginalized women and girls and those subjected to GBV. The design of technologies must address these vulnerabilities and acknowledge that women and girls may be accessing technologies in unsafe spaces.⁵⁸ These aspects may otherwise not be captured during user testing or factored into design.

Increased awareness of technology safety and security systems for people and organizations, including for developers, is critical. Technology developers should be aware that control features such as customized privacy and sharing settings as well as filtering, blocking, favouriting and



Increased awareness of technology safety and security systems for people and organizations, including for developers, is critical

reporting functions can have unintended consequences, including increased surveillance, for marginalized and vulnerable groups. This does not mean that they should not be available as options, but neither should they be the default for all users. Transparency, usability and choice are imperative so that individuals can tailor technology to their specific circumstances. Importantly, State or company surveillance does not equate to safety.⁵⁹ Other safety measures may have exclusionary and problematic effects. Age verification techniques are often said to be useful in protecting young people from harmful digital content but can be overapplied to young people wanting access to SRH information. Implementing age verification techniques can also violate children's privacy and data protection rights.

Those administering digital and machine applications and technologies must be aware of and engage security systems to protect data, privacy and rights, without adverse effects on users. Further, technological applications have unknown backend data collection practices that are difficult to grasp for many end-users, an issue exacerbated when creating products for use in low-literacy and low-numeracy environments. Relying on end-users to identify data protection concerns and/or outline how

Those administering digital and machine applications and technologies must be aware of and engage security systems to protect data, privacy and rights

technology may be hacked and used for nefarious purposes is not a burden that should lie with users.⁶⁰ Governments and tech companies should include considerations of data privacy in the ideation phase, reimagining new business models and policies that do not bring tech products to populations with low digital literacy in exchange for their data. Further, rather than having opt-out functions in relation to privacy and data-sharing, there should be opt-in requirements to share user data and information. To navigate this issue, users need easy-to-read information about policies, processes, and device and platform features. Assumptions are often made about what constitutes accessible instructions and functionality, including in relation to cognitive or intellectual disability.⁶¹

While data protection laws are gaining traction globally, a range of considerations must be taken into account, including the danger of broad or inappropriate exemptions; the importance of implementing both privacy and data protection regimes; the requirement for data protection authorities to be structurally and substantially independent; and the extent to which data protection regimes can be helpful in ensuring transparency and accountability in government and private sector use of AI via automated decision-making systems.⁶²

Furthermore, there is a lack of diversity in the technology industry, especially in positions of innovation, leadership and cybersecurity.⁶³ Globally, a large number of women and people from lower-income and marginalized communities, and from culturally and linguistically diverse settings, are employed formally and informally in the industry. Their roles are at the beginning and end of the technology supply cycle, however, as miners of basic and rare earth minerals; factory workers in refineries and manufacturing plants; providers of programming, content moderation and data labelling (for AI); customer service representatives; and managers of e-waste.⁶⁴ Women and girls provide ancillary labour that informally supports the industry and bear the costs of accompanying environmental devastation and social and economic instability (including GBV and trafficking). Remarkably, this global diversity is rarely reflected in decision-making and innovation.

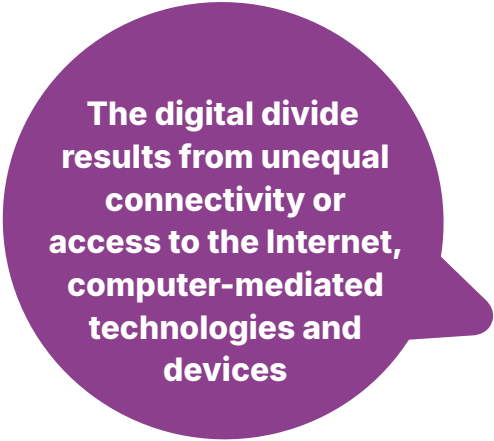
The result is a range of products and services reflecting the needs and priorities of a narrow range of users who most closely resemble the top levels of the industry, rather than its global diversity. This has resulted in a failure to meaningfully consider the needs, vulnerabilities, interests and rights of *all* users, and led to discriminatory hierarchies and dangerous digital environments for women and girls. Equality-focused design and implementation principles are often lacking.⁶⁵ The lack of women in tech can in fact lead to poorer service quality for all people but particularly women as well as reduced opportunities for women. In health care, these biases can be life threatening.⁶⁶ Expanding leadership, innovation and cybersecurity teams within the tech industry through a significant investment in the education, employment and entrepreneurship of women is a transformative opportunity.⁶⁷

In short, compliance with safety-by-design principles and processes builds safety and security into technology from the outset, supporting the use of technology for its intended purposes.

Deployment of technology: digital inclusion

Given that technology is built for dominant and largely homogenous communities that may idealize interactions, its design does not consider the diversity and complexity of human beings, including power imbalances and inequitable access. Shifting from the design of technology to the deployment phase brings the heterogeneity of “users” into the spotlight, a critical component of mitigating risks and harms, and providing equitable access to technology and its benefits for all users. For this think piece, technology deployment is the process through which the product is delivered to customers and end users.





The digital divide results from unequal connectivity or access to the Internet, computer-mediated technologies and devices

The heterogeneity of end-users is increasingly reflected in research on the digital divide, which affirms the gap between those who have access to and use technology, including Internet connectivity, and have digital literacy skills and Internet-enabled devices, and those who do not. The digital divide results from unequal connectivity or access to the Internet, computer-mediated technologies and devices, and differing digital skill sets. Discrepancies in technology access, uptake and ownership have been particularly apparent for populations at the intersection of multiple forms of discrimination, including in relation to gender identity, disabilities, ethnic and cultural identity, education, age and geographic location.⁶⁸

Recognizing that technology can accelerate the goals of the Programme of Action, it is important to understand and address how technology is used differently by various communities and age cohorts, and the barriers they experience. Digital transformation benefits are not equally balanced throughout society; this is most apparent in the gender digital divide, which is both a consequence and a cause of violations of women's and girls' human rights. Social attitudes and wider structural and systemic barriers (such as gender inequality and localized social constraints) limit or discourage the use of digital media and devices. Men are likely to have greater opportunities to use technology and develop digital skills than women, including through schools, workplaces and their greater presence in public spaces and community socializing.

The most recent data published by the Global System for Mobile Communications Association (GSMA)⁶⁹ show that more women in low- and middle-income countries are using the mobile Internet than ever before. But their rate of adoption has slowed for the second year in a row, and a significant gender digital divide persists. Women are 19 per cent less likely than men to use the mobile Internet. Of the 900 million women still not using it, almost two thirds live in South Asia and sub-Saharan Africa, where mobile gender gaps are widest. The GSMA research also identified the top three barriers preventing women from adopting the mobile Internet, even if they are aware of it and are mobile users. These obstacles comprise affordability (primarily of handsets), digital literacy and skills, and safety and security.

Rapid uptake of technology is occurring among young women around the world. Given the high proportion of youth populations in some regions, there may be more rapid uptake in some countries, including in Africa. While an estimated 69 per cent of 18 to 24 year olds globally are online using mobile or broadband Internet, however, only 38 per cent of them are online in the least developed countries. Two thirds of young people (2.2 billion) do not have Internet access at home.⁷⁰

Population ageing is occurring in all regions and countries. Data about older women's use of technology are scant but their uses and uptake of technology lag those of younger cohorts. Gaps are exacerbated for older women with disabilities, gender and sexually diverse older adults, and older adults residing in the Global South, who statistically have less access to technologies. Low access to technologies, connectivity and digital literacy amplifies the vulnerabilities and marginalization of older adults, including through online fraud and scams.⁷¹

Factors affecting access and use of technologies

Availability

Weak Internet connectivity and ICT infrastructure reduce digital access. Limitations in the electricity supply and 3G/4G or broadband coverage, low quality-of-service regulation and an absence of safe or free access points, for example, diminish the availability of the Internet and ICTs.⁷² Further, meaningful connectivity depends on an understanding that not everyone connects to the Internet in the same way. A sole reliance on a binary metric of connectivity may exacerbate inequalities online and offline. To adequately address meaningful connectivity, “a user’s connection must be reliable, of sufficient bandwidth, and with a low enough latency to enable them to experience the wealth of the internet’s potential.”⁷³

Affordability

Connectivity, infrastructure and devices can be more expensive in the Global North compared to the Global South. Countries with more resources are likely to reap the benefits of technologies. High costs are major obstacles to access, particularly for women and adolescents. These are expected to grow as the expense of owning and operating technologies rises alongside technological sophistication and functionality. High data costs can restrict Internet content to those with sufficient data allowances.

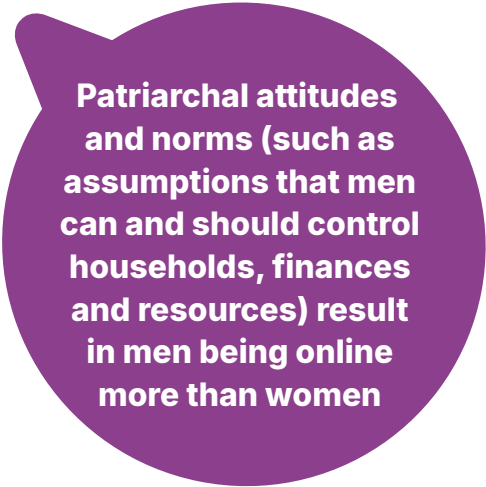
In many regions, a gender pay gap leaves women economically dependent on men or without enough control of household finances to access technology. Women, especially those in poverty, report having limited time to use technologies as they need to work long hours, including to provide unpaid care.⁷⁴

Sociocultural barriers

Sociocultural barriers persist across the socioecological model at the individual, community and structural levels. At an individual level, women may experience a denial of access to the Internet or devices as part of a continuum of coercive control exercised by an intimate partner or other family member. At a community level, patriarchal attitudes and norms (such as assumptions that men can and should control households, finances and resources) result in men being online more than women. Men may have more mobility and cultural freedom to use facilities such as public or private places with Internet access. Family support enables technology adoption but women and girls may be discouraged or prohibited from using the Internet by their families or other gatekeepers.⁷⁵ This may be particularly the case for women and girls with disabilities.⁷⁶

Women with higher levels of education typically have greater confidence in their abilities to use technologies. Yet access to higher education is uneven and so is the confidence of women in using technology. Older women, for whom technology was not embedded in formative education curricula, are marginalized due to a lack of digital literacy.⁷⁷

At a structural level, insufficient awareness of different norms dictating access to devices and meaningful connectivity will deepen those inequalities. Greater connectivity will provide dominant



Patriarchal attitudes and norms (such as assumptions that men can and should control households, finances and resources) result in men being online more than women

groups in a community with increased access to information and employment opportunities. More vulnerable groups, such as those without access to devices, will become further marginalized.

Privacy, security, trust and safety risks

Women and girls must be able to safely use technologies to enable digital inclusion. The GSMA research indicates that safety concerns are one of the top three barriers preventing access to connectivity.⁷⁸ The burden of protecting their rights, well-being and security all too often falls on women and girls. Given the drivers of violence and structural inequalities, this is arguably a never-ending, impossible task.

Concern about women's and girl's online safety may result in their hesitation to use the Internet or in community-based, familial or other norms forbidding use altogether. These tendencies could be motivated by fears that digital technologies can expose women and girls to grooming, sextortion, sexual trafficking, harassment, stalking and other forms of harm and violence.⁷⁹ Distrust and lack of safety come at an opportunity cost in terms of increased literacy and empowerment.

Even where access and meaningful connectivity are supported, TF GBV⁸⁰ may push women from online spaces. Recent studies indicate that closing the gender digital divide correlates with an increase in the experience of TF GBV.⁸¹ TF GBV carries significant health, safety, political and economic consequences for women and girls, their families and communities, and society as a whole. A recent survey conducted by the United Nations Educational, Scientific and Cultural Organization, working with 901 journalists in 125 countries, found that 73 per cent of women journalists had been subjected to online violence and 20 per cent were attacked offline as a direct



consequence of online violence.⁸² A global study by the Inter-Parliamentary Union revealed that 41.8 per cent of women in politics had seen images or comments with sexual, defamatory or humiliating connotations of themselves being disseminated through social media; 44.4 per cent had received threats of “death, rape, beatings or abduction during their parliamentary term”.⁸³ As women and girls self-censor to prevent TF GBV, their voices are silenced, contributing to deepening inequality.

Relevance of digital content, applications and services

Women are more likely than men to report that Internet content, applications and services have limited relevance, benefit or usefulness for their lives. The lack of content in local languages also significantly hinders access to meaningful and relevant content online, impacting educational and personal development opportunities. Alarming, engagement with material, software and programmes that speak to their lived and diverse realities may be censored or blocked by States. Low awareness of digital services reduces uptake, reach and effectiveness.⁸⁴

Business models of technology

Technological innovation and the business models that drive it have altered lives and communities around the world. As highlighted above, business models are propelled by competition, perceived markets and profit motives, which influence corporate conduct and technology design decisions in ways that contribute to human rights violations, threaten democratic values and exacerbate inequalities.⁸⁵ For example, competition can compel a rush to bring products to market before negative safety implications are fully vetted. Competition among companies can prevent the sharing of strategies that counter harms and protect safety. Profit motives can deprioritize safety and privacy protections in favour of technological novelty or the reuse of valuable, sensitive data. To harness the potential of technology, rights-based regulations must be established and enforced, ensuring due diligence to prevent and mitigate harm and enable systems of accountability and redress.⁸⁶ To create regulatory spaces that protect the rights of women and girls, it is important to outline ways in which business models operate.

In the case of technology, data intelligence informs and enables ideal and constantly evolving and improved interaction with customers or users to increase use and engagement, thereby enhancing profitability. Data generated through technology also form a secondary commodity that can be traded for profit. The global diffusion of digital technologies is radically increasing the amount of data created about the online and offline activities of individuals and communities. The volume of data, as digital technologies expand, continues to increase exponentially, from 2 zettabytes over the last decade to 64.2 zettabytes in 2020, with that figure expected to grow to more than 180 zettabytes by 2025. This represents enormous market opportunities.⁸⁷ The vast majority of data is visible or accessible to individuals but is stored and managed by companies, governments and administrative actors for their own purposes.

Shareholder primacy and profit incentives in large technology companies have reinforced incentives for data hoarding and trade



The global diffusion of digital technologies is radically increasing the amount of data created about the online and offline activities of individuals and communities


to extract value from data, often counter to the interests and benefits of individuals. Consumers of online goods and services are often not aware that their digital interactions generate data through movement, communication, political engagement, shopping and accessing public services. They may also not realize the value of these data.

Given that individuals are often unaware of data held about them, by whom or how data are used, they are often trading personal data for access to digital infrastructure without the knowledge or consent that data are being commodified by a third party. This model rewards businesses that establish efficient and invisible mechanisms to generate, use, analyse, share and sell consumer data to third parties. A compounding concern is the limited ability of individuals to anticipate and mitigate digital security risks that accompany the proliferation of personal and non-personal data. This problem is magnified for marginalized groups and individuals with limited access to digital technology and low levels of digital literacy, including women and girls. It also presents unique threats to survivors of GBV or women at risk of GBV.⁸⁸ The potential to undermine the Programme of Action by increasing the vulnerability of users, particularly those with low levels of digital literacy, is manifold.

Digital transformation is taking place across private and public sectors, where the “datafying” of citizenship and civic engagement continues to expand. Datafication describes the turning of many aspects of our lives into data and subsequently information of value. Public registration, receipt of services or participation in political processes increasingly create data that are not visible or accessible to individuals. The proliferation of smart devices and the Internet of Things represents the greater ubiquity and opacity of these dynamics, as everyday devices increasingly transmit data about their use and environment to manufacturers and third parties without users’ awareness or consent.⁸⁹

Being unaware of what data are generated, who holds them and how they are used and shared limits individuals’ capacity to shape those interactions and may put them at risk. This may result in individual life-threatening harm as a result of doxing (the searching for or publishing of private information about a person on the Internet, including human rights defenders) or the use of data to identify survivors of conflict-related sexual violence or adolescents accessing SRHR services in highly restrictive contexts. Macro harms may occur, whereby data are used to target populations who have accessed information relating to sexuality online. Given the comparatively lower levels of digital literacy among women and marginalized groups, they are most exposed to risks of harm, including, for example, reduced access to SRHR or exposure to stigma for accessing SRH and GBV services in certain contexts.

Data as a commodity means that in a world where physical and digital identities are inextricably linked, an embodied approach to data governance and a holistic understanding of bodily autonomy and integrity, dignity and freedom that spans the digital and physical spaces are critical. For example, consent-based frameworks must be viewed through a prism of relational autonomy rather than individual autonomy, in that conditions must be created for informed data ownership at the individual level before consent can be given for



Conditions must be created for informed data ownership at the individual level before consent can be given for data use

data use. In some settings, the requirement for digital identification for vulnerable populations has raised significant concerns, since the provision of informed consent is questionable when no other options are available to access life-saving services.

The mandatory use of biometrics for identification, often without adequate safeguards or consent, poses risks of privacy infringement and potential misuse. In certain countries, these data have reportedly been used for purposes beyond identification, including surveillance and control, leading to ethical and human rights concerns. While such data might support increased understanding of population needs or movements and the tailoring of services, they also pose serious risks to the well-being and rights of individuals. The lack of transparency and accountability in how sensitive information is handled exacerbates the vulnerability of already marginalized groups.⁹⁰



The lack of transparency and accountability in how sensitive information is handled exacerbates the vulnerability of already marginalized groups

One of the most lucrative Internet business models is the collection and sale of personal data, which are used to target people with online advertisements. Advertising, the heartbeat of the Internet, allows users to access a wide range of services and information in exchange for attention or data. This business model has given rise to an opaque and complex industry where the collection and commodification of personal data have become extractive and exploitative, and largely occur without user consent. A recent gendered analysis of how women's reproductive milestones are used for microtargeting purposes demonstrates how data promote false stereotypes associated with childbearing.⁹¹ These stereotypes are detrimental to women's rights and well-being. Further, the online advertising ecosystem denies women full sovereignty over their health data, and by design, puts women in a perpetual state of vulnerability. Risks to the well-being of women and girls as a result of harmful advertising impede progress on the Programme of Action, particularly given the increased uptake of technology.

This set of concerns was reflected recently in a survey of 1,000 women and FemTech users across the United Kingdom. Findings revealed that 82 per cent of women were unclear about how reproductive apps were safeguarding users' data, while over 60 per cent showed great distrust in the ability of these apps to safeguard their privacy. Approximately 44 per cent had deleted an app due to privacy concerns and at least 20 per cent had deleted a menstruation or fertility app. While the use of technology to increase access to information and services may have the hallmarks of successfully reaching the furthest behind, significant concerns around safety and data protection have prevented full uptake. At least among users in the United Kingdom, there is increased recognition of how tech, even if designed for good purposes, may expose users to harm as a result of insufficient assurances around data ownership.⁹²

The use of data collected across social media platforms promotes an engagement-driven, content-agnostic model. The longer users engage with a platform, for example, the more data can be collated against a user profile. This model means that harmful, shocking and misogynistic content, which generates increased engagement, is likely to be more rapidly propagated, thereby deepening harmful norms. Algorithms used to promote content and increase engagement are relying on data produced as users engage. Given that 70 per cent of content generated on YouTube, for example, is recommended by algorithms,⁹³ a cycle of proliferating harmful content manifests in user platforms. Anti-rights content and mis/disinformation is permitted to flourish and is propagated



across platforms at an alarming rate while positive, rights-based and gender-transformative content receives less uptake in terms of viewing or readership.

Metadata are another sensitive but nearly invisible type of data. They are collected in the background of digital activities. Such data can include the length of time spent on a site or app, the geolocation of the user during the use of an app or beyond, other apps on a device, times and dates of communications, other parties to a communication, and more. Metadata can also include the type of device, its operating system, telecommunications provider or Wi-Fi network, and usage patterns, all of which contribute to a “fingerprint”, with concerning implications in terms of the unique identification of a user, even when they have not voluntarily supplied personally identifying information. Data privacy protections must be in place for obviously sensitive data and for metadata.

Personal data, beyond being used for profit, can also be traded at very little cost for use by malicious actors, including groups intent on spreading disinformation and misinformation on SRHR. For example, in May 2022, a media outlet purchased aggregated location data from a data broker, SafeGraph, that indicated how many people were visiting family planning centres, how long they were there, where they were before they went there, and where they went after they left, for the price of \$160.⁹⁴ While these data could be used for evidence-based programming to increase access to rights and choices for women, they may also be deployed by malicious actors to fuel targeted disinformation campaigns.

As highlighted in the preceding section, the design of technology, which permits opportunities for data collection, poses the same risk of harm regardless of whether intentions behind the technology were good or malicious. Maintaining control over data, including personal and intimate information, is paramount, particularly where people using digital technologies are vulnerable, in order to prevent exploitation, harm and deepening inequality.⁹⁵ It is also important to recognize the mosaic effect, when multiple data sets are linked to reveal significant new information. This process can be leveraged for increased insights as well as significant harm.⁹⁶

Such imbalances disempower individuals and reward societal harm. They have prompted widespread dissatisfaction and increasing calls to rethink the foundational structures of today's data economy. There are, however, no clear market incentives for an alternative organizing principle, although a Massachusetts Institute of Technology-supported project initiated by Sir Tim Berners-Lee (the "father" of the worldwide web) has proposed a new model in which individuals own their own data.⁹⁷ A fundamental redesign of how the emerging data economy will function is critical to address the inherent tension between individual human rights and economies.

Privacy-by-design principles are key. These require users, including women and girls, to be fully informed about and able to provide informed consent or able to refuse consent to policies and user agreements. They should have the power and autonomy to make decisions about their data in their best interest. Opt-in functionality as opposed to opt-out of data sharing is a central feature of privacy-by-design.⁹⁸ The principles of data feminism can be a helpful framework, including to examine power, consider context and make labour visible.⁹⁹ Control over data endows women and girls with agency, is crucial for managing their safety, lowers the administrative burden and increases the quality of data for stakeholders.¹⁰⁰

Data must be conceptualized as a right attached to an individual, as an extension of the person, with bodily autonomy in the foreground (see also Box 5). A human-centric model for data intermediation emphasizes that people must have direct control over the data they generate through their everyday interactions. This model is increasingly adopted by private and public sector organizations. It strengthens personal privacy while empowering women and girls to leverage their data to create economic and social value. Data sovereignty, also known as digital sovereignty, is proposed as a framework to support a rights-based and deliberative approach to data.¹⁰¹

Direct control over personal data can strengthen health outcomes and employment opportunities and reduce the effort and transaction costs required to manage finances, health care and public services. It can provide a foundation for empowering people in terms of their health and well-being, including those who are most marginalized. Economic and technical models built on principles of human-centricity and individual control empower everyone but the benefits are often most profound for the least capacitated. Clear control over medical data may be most powerful for the chronically ill; control over benefits data may be most significant for the economically and

BOX 5

Accounting for the impacts of data sharing on communities

Although not discussed in detail in this paper, recognition of colonial practices in data collection must also be considered. Indigenous-led data sovereignty and data governance policies provide guidance on how data should be viewed, generated and collected, and the need to centre Indigenous peoples' rights to self-determination, autonomy and ownership of data. Crucially, this includes shifting the conception of data rights as solely the rights of individuals towards an accounting for the impacts of data sharing on entire communities and populations. Efforts to ensure communal data rights move beyond a deeply embedded Western scientific assumption of individuality that also underpins technology design.

Source: Lovett and others 2019; UN OHCHR 2022; WHO 2021; World Bank 2021.

politically marginalized. While there is tremendous promise in leveraging technology for universal health coverage, this will require smart, context-specific policies and programming with ample flexibility to adapt as needs and opportunities change, and with robust safeguards to protect privacy, data security and equity. The health sector, which by nature is data intensive, lends itself to the use of technology for analytics to improve health outcomes, respond to public health crises, and efficiently and equitably allocate resources.¹⁰²

A human-centric model increases protections against data mismanagement, leaks or misuse by third parties and must be safeguarded and regulated through appropriate legal provisions. The everyday value of data empowerment can be manifest in mundane aspects of life, such as shopping or entertainment, but is most profound for data that are deeply sensitive and personal. This is particularly the case for data relating to health treatment and case management and responses to GBV.¹⁰³

Clear data governance systems that protect the rights of users, including with the use of encryption and anonymization (where relevant), while supporting innovation in technology are vital.¹⁰⁴ It is imperative that non-government, government and private organizations securely collect and manage data. It is widely acknowledged that systems of governance, including data governance, need to be reimagined.¹⁰⁵ The Lancet and Financial Times Commission on Governing Health Futures highlighted that “the governance of digital technologies in health and health care must be driven by public purpose, not private profit”.¹⁰⁶ The commission called for “a new approach to the collection and use of health data based on the concept of data solidarity, with the aim of simultaneously protecting individual rights, promoting the public good potential of such data, and building a culture of data justice and equity”.¹⁰⁷ There should be strict protocols on access to data and compliance with standards and guidelines for data management and access. Data must be stored in secure servers with timelines for data destruction.¹⁰⁸

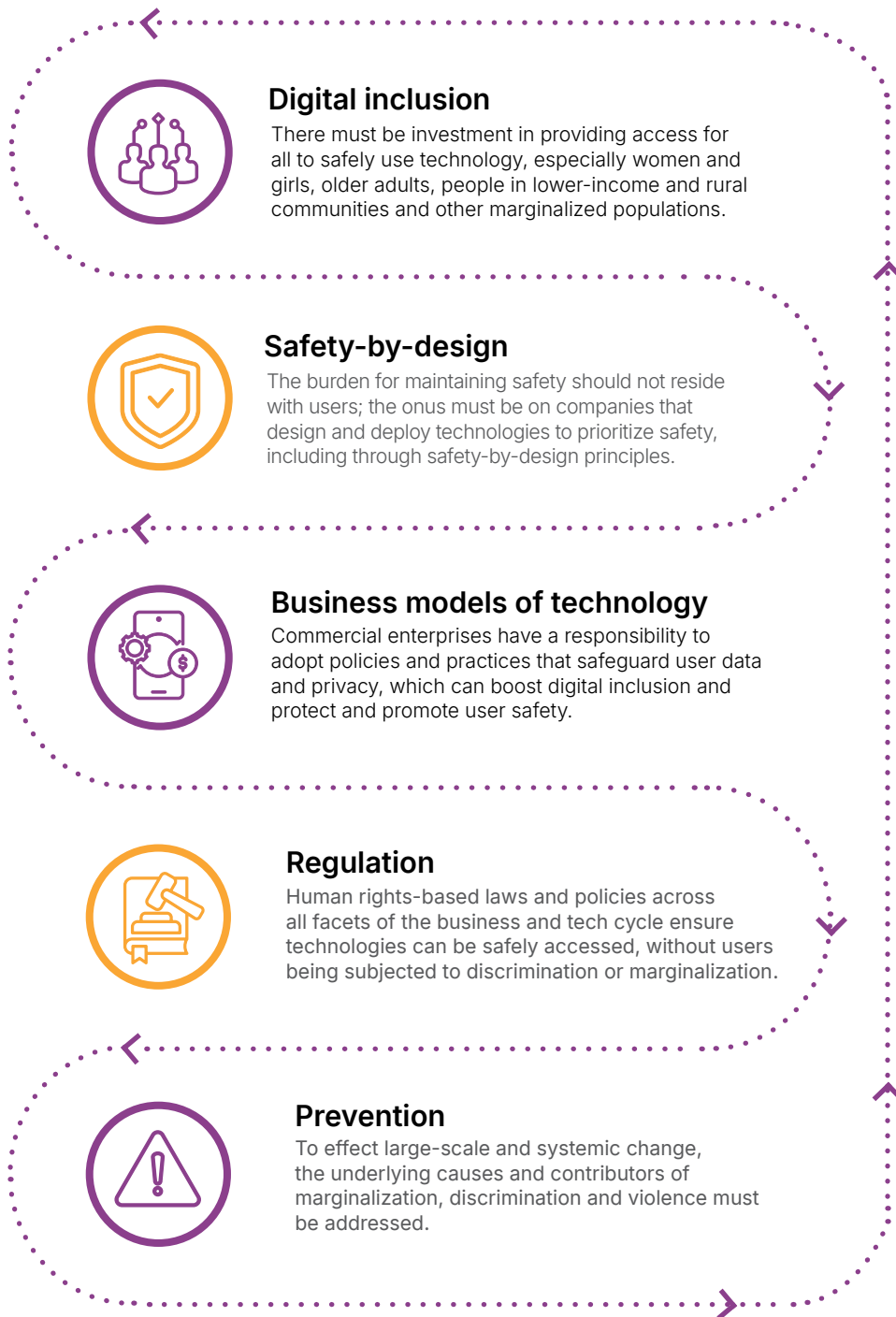
While the interaction of women and girls with technology will and should continue to increase, data protection and privacy should be a priority in ensuring that women and girls are not further exposed to harmful actors who mine personal data for malicious actions. Business models for technology require reconsideration and innovation to anchor data collection, storage and use in safe and ethical principles as well as human rights-based approaches. This will be central to making concerted and productive progress towards the Programme of Action.

4 | Recommended Actions

The path forward is fraught, unclear and uncertain, but one upon which we must embark together (Figure 2). Recognizing that the digital world is a space that all populations increasingly occupy, it must reflect the principles and ambitions of the ICPD Programme of Action as opposed to perpetuating a status quo of harmful norms and inequalities. Technologies can be imagined and reimagined as a critical channel for achieving the ambitions of the Programme of Action if there is coordination and cooperation among organizations in government, civil society, academia and private industry. Silos must be bridged, across sectors and movements, with research and standards shared and rights upheld around the world.

▶ **FIGURE 2**

The pathway forward is fraught and uncertain, but one upon which we must embark



A safe digital future

Investment in safe and secure technology built on principles of data privacy along with rights-based regulations are crucial for the meaningful digital inclusion of women and marginalized populations. Only with ethical business models can digital technology accelerate the achievement of the ICPD Programme of Action.

The following recommendations reflect the United Nations Guiding Principles on Business and Human Rights, underpinning a shared responsibility of businesses, governments and civil society. The three pillars of this model are: first, States have a duty to **protect** against human rights abuses by businesses through policies, regulation and adjudication; second, there is a corporate social responsibility to **respect** human rights, act with due diligence to avoid infringements and address adverse impacts on human rights; and third, there must be access to effective **remedy** for victims through judicial and non-judicial grievance mechanisms.¹⁰⁹

The recommendations reflect the structure of this paper. They are addressed to a range of stakeholders to bolster digital inclusion in the design and deployment of technologies and regulation. Recommendations include encouraging investment in alternative technology business models that promote and protect human rights. In this way, uptake of technology can be increased, safety and privacy prioritized and protected, and harms and risks prevented and mitigated. This will ensure that the world benefits from digital transformation.

Digital inclusion

To realize the benefits of digital technologies, it is paramount that all users can access technology and are equipped to navigate it safely. In particular, there must be investment in providing those with less uptake, including women and girls, older adults, people in lower-income and rural communities and other marginalized populations, with access, privacy protections, digital literacy education and resources about privacy and tech-safety. Significant investment must be directed towards:

- ▶ Equitable availability of and access to technology and supporting infrastructure, including meaningful connectivity.
- ▶ Investment in digital literacy and education for users of all ages and in all their diversity, to build the necessary skills and confidence for navigating technology safely and in an informed manner.
- ▶ Ongoing investment in social and gender norm change to ensure individual, community and systemic endorsement of equitable access to technology.

Safety-by-design

Providing information about and support for users on digital safety is vital to enhancing digital inclusion. The burden for maintaining safety should not reside with users alone, however; the onus must be on companies that design and deploy technologies to prioritize safety through safety-by-design principles. Global rights-based approaches to safety-by-design require participatory design, accountability to users, non-discrimination and equality in access and use as well as the empowerment of users and robust underlying legal systems.

Safety, security and privacy must be considered from inception and directly incorporated throughout the design and deployment stages. To identify and proactively mitigate or prevent risk and harm, all users, especially marginalized and vulnerable ones, must be actively engaged. Additionally, for technologies to reflect a broader spectrum of perspective and need, there must be efforts to diversify leadership and innovation teams within the tech industry. The make-up of the tech industry and safety-by-design process must be intersectional and trauma-informed. These principles can be accomplished through:

- ▶ Increased investment in national, regional and international technology industry standard-setting bodies to support compliance with safety-by-design.
- ▶ Support for special measures, including affirmative action, to ensure that the design and development of technologies and platforms (including safety features and moderation mechanisms) is in partnership and with the participation of users in all their diversity as well as researchers, civil society organizations, front-line TF GBV service providers and rights-based advocates. Consultation and co-design of software, devices and applications should occur at the individual, family and community levels.¹¹⁰
- ▶ Empowering users in their interaction with technology through usable and accessible features and options for consent (or for declining consent), including to opt-in to data collection and sharing as opposed to default opt-out architecture.
- ▶ Programmes to recruit and initiatives to support and retain women and other marginalized populations, in all their diversity, in leadership, innovation and security teams throughout the technology sector.
- ▶ Investment in tertiary education to integrate safety-by-design principles as well as practical exercises into the curricula of a range of disciplines, including computer science, technology, engineering and law.
- ▶ Integration of safety-by-design principles in technology education programmes in schools and university curricula.
- ▶ Transparency and reporting requirements for the technology sector relating to design, deployment, data security and privacy, and moderation, using human rights frameworks and rights-based law reform.

For practical guidance and actionable recommendations, see the outcomes and recommendations of the report *Tech Policy Design Lab: Online Gender-Based Violence and Abuse*;¹¹¹ *UNFPA's Guidance on the Safe and Ethical Use of Technology for GBV and Harmful Practices Interventions*;¹¹² and the raft of guidelines, tools and recommendations of the Australian eSafety Commissioner.¹¹³

Business models of technology

Commercial enterprises have a responsibility to adopt policies and practices that safeguard user data and privacy, which can boost digital inclusion and protect and promote user safety. While business models will prioritize profit, technology as a public good requires regulation and innovation to protect and promote the human rights of users and the well-being of society more broadly. This involves:

- ▶ Investment in innovation to grow alternative business models that reduce reliance on the commodification of personal data, thereby protecting users' safety and security.
- ▶ Support for the design of technology, including AI models, through partnerships between governments and academia, as a public good reflecting standards and protections required to support safe, equitable access and use.
- ▶ Increased transparency of data economies, including among third-party organizations trading in data, to enable effective regulation.

- ▶ Partnership between governments and technology companies to enable the regulation of safety and security by design and equitable access to create products as public digital goods rather than as public relations or advertising devices.¹¹⁴
- ▶ Transparency and reporting requirements to inform the accountability of business and tech relating to design, deployment, data economies (including the sale of data and registers of data brokers), data security and privacy, and moderation processes.
- ▶ Implementing and enforcing robust governance mechanisms, including laws, regulations, oversight and enforcement, to ensure the safety and privacy of users, particularly women and girls on the margins.
- ▶ Ensuring rights-based law reform to enable and empower regulatory bodies to be sufficiently adaptable and flexible (while remaining rights-based) to address harms as a result of rapidly evolving technologies and unforeseen risks.

Monitoring and regulation of business operations, by States and international bodies, and sanctions for contravening policy and laws can aid compliance with these recommendations.

Regulation

Human rights-based laws and policies across all facets of the business and tech cycle are vital to ensure that technologies can be safely and inclusively accessed and used, and that they protect user rights and avoid deepening discrimination and marginalization. This requires States and international bodies to institute rights-based laws or law reform to support independent regulatory mechanisms. Laws and regulations should:

- ▶ Embed systems of safety, security and privacy across corporate standards that can be enforced by legislation.¹¹⁵
- ▶ Enable the protection of user rights to personal data, including through data collection, management and governance.
- ▶ Enact codes of conduct and standards around digital advertising.
- ▶ Consider gender-transformative access to and use of technologies including through investment in meaningful connectivity and education.¹¹⁶
- ▶ Enable proactive prevention, mitigation and responses to harm, including TF GBV.¹¹⁷
- ▶ Divest regulatory powers to an independent national regulator to ensure the accountability of business and tech as well as to lead investment in research and community-based interventions.
- ▶ Consider incentives for private sector compliance with law and policy as well as financial and operational penalties for non-compliance.¹¹⁸
- ▶ Take into account the global nature of technology in the development and enforcement of national legislation.

Prevention

Response efforts are important, but to effect large-scale and systemic change, the underlying causes and contributors of marginalization, discrimination and violence must be addressed. This involves:

- ▶ Scaling up investment in programmes to address harmful social and gender norms at a community and structural level to transform access to and use of technology.
- ▶ Increased and targeted investment in the education of women in all their diversity and other marginalized groups, including in science and technology to ensure that technology reflects a broader spectrum of users.
- ▶ Investment in action and strategies to support anticipatory, pre-emptive prevention of disinformation campaigns, including infodemics.
- ▶ Building and extending partnerships and networks across regulatory bodies, digital rights movements, businesses and tech, governments, survivor advocates, academia and communities to ensure a shared vision for safety in technology and proactive moves to pursue this.
- ▶ Strengthening research that supports evidence on the positives, limitations, consequences and risks of technologies, and the commodification of personal data, on all cohorts, including marginalized and vulnerable populations.
- ▶ Diversifying leadership, innovation and cybersecurity teams within the technology industry, while attending to gendered environmental and social issues in all parts of the technology supply cycle.

5 | Conclusion

- ▶ In highlighting key findings and recommended actions for a safe digital future, this think piece has shown that investment in safe and secure technology, built on principles of data privacy and users' consent along with rights-based regulations and equitable deployment, is crucial for the meaningful digital inclusion of women and marginalized populations.
- ▶ Only with design, deployment and ethical business models can digital technology accelerate the achievement of the ICPD Programme of Action.



References

- Abdenur, Adriana Ertha and Lycia Brasil, 2019. "Migration and Technology: Lessons from the Brazil-Venezuela Border." Pass Blue Independent Coverage of the UN, 25 July. Website: www.passblue.com/2019/07/25/migration-and-technology-lessons-from-the-brazil-venezuela-border, accessed 3 April 2024.
- Aceng, Sandra, 2023. "How Women of Uganda Network (WOUGNET) Uses Technology to Respond to Online Gender-based Violence." In *Technology and Domestic and Family Violence: Victimization, Experiences and Responses*, Bridget Harris and Delanie Woodlock (eds), 186–191. London: Routledge.
- Adegoke, Damilola, 2022. "Youth Digital Exclusion, Big Data Divide and the Future of Work." In *Youth Exclusion and Empowerment in the Contemporary Global Order: Existentialities in Migrations, Identity and the Digital Space*, Ákánle Oláyinká (ed), 33–47. Bingley, UK: Emerald Publishing Limited.
- Alaoui, Fatima Z. Chrifi, 2015. "The Arab Spring between the Streets and the Tweets: Examining the Embodied (e)Resistance through the Feminist Revolutionary Body." In *Women of Color and Social Media Multitasking: Blogs, Timelines, Feeds, and Community*, Keisha Edwards Tassie and Sonja M. Brown Givens (eds.), 35–67. Lanham, MD: Lexington Books.
- Alencar, Amanda, 2023. "Technology Can Be Transformative for Refugees, but It Can also Hold Them Back." Migration Policy Institute, 27 July. Website: www.migrationpolicy.org/article/digital-technology-refugees, accessed 3 April 2024.
- Alliance for Affordable Internet, 2020. *Meaningful Connectivity: A New Target to Raise the Bar for Internet Access*. Washington, DC: Alliance for Affordable Internet.
- Andere, Bridget and Megan Kathure, 2023. "Strengthening Data Protection in Africa: Key Issues for Implementation." Access Now. Website: www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf, accessed 3 April 2024.
- Anderson, Monica and Jingjing Jiang, 2018. "Teens, Social Media and Technology 2018." Pew Research Centre, 31 May. Website: www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018, accessed 3 April 2024.
- Anwar, Asia Abdelkarim and others, 2023. "Digital Violence against Women in Iraq." SecDev Foundation. Website: portal.salamatmena.org/wp-content/uploads/2024/01/Iraq-DVAW-2023-EN.pdf, accessed 3 April 2023.
- APC (Association for Progressive Communications), 2018. "Providing a Gender Lens in the Digital Age: APC Submission to the Office of the High Commissioner for Human Rights' Working Group on Business and Human Rights." APC. Website: www.apc.org/sites/default/files/APC_submission_Providing_a_gender_lens_in_the_digital_age.pdf, accessed 3 April 2024.
- Athar, Rima, 2015. "From Impunity to Justice: Improving Corporate Policies to End Technology-related Violence against Women – A Summary." Association of Progressive Communication (APC). Website: www.apc.org/sites/default/files/Impunity_Athar_Summary.pdf, accessed 3 April 2024.
- Auxier, Brooke and others, 2020. "Parenting Children in the Age of Screens." Pew Research Centre, 28 July. Website: www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens, accessed 3 April 2024.

- Benjamin, Ruha, 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK: Polity Press.
- Bernal Aparicio, Cristina and Siope Vakataki 'Ofa, 2021. "Digital Technologies for Climate Change Adaptation in Asia and the Pacific." Working Paper Series. Bangkok: United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), Information and Communications Technology and Disaster Risk Reduction Division.
- Borges do Nascimento, Israel Junior and others, 2022. "Infodemics and Health Misinformation: A Systematic Review of Reviews." *Bulletin of the World Health Organization* 100(9): 544–561.
- Broadband Commission Working Group on Broadband and Gender, 2013. *Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society*. Geneva: United Nations Educational, Scientific and Cultural Organization (UNESCO) and International Telecommunications Union (ITU).
- Caravan Studios, 2024. "Our Methodology." Website: www.caravanstudios.org/methodology, accessed 3 April 2024.
- Carlson, Eric L., 2006. "Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow." *Elder Law Journal* 14: 423–452.
- Cavoukian, Ann, 2011. "Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices." Toronto, ON: Information and Privacy Commissioner of Ontario.
- Ceia, Vanessa and others, 2021. "Gender and Technology: A Rights-based and Intersectional Analysis of Key Trends." Oxfam Research Backgrounder Series. Boston, MA: Oxfam America.
- Center for Countering Digital Hate, 2022. "Deadly by Design." Website: counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf, accessed 3 April 2024.
- Centre for Humdata, 2020. "Exploring the Mosaic Effect on HDX Datasets." Blog, 22 July. Website: centre.humdata.org/exploring-the-mosaic-effect-on-hdx-datasets, accessed 3 April 2024.
- Chair, Chennai and Ariane De Lannoy, 2018. "Youth, Deprivation and the Internet in Africa." After Access Policy Paper No. 4. Cape Town: Research ICT Africa.
- Chang, Emily, 2019. *Brotopia: Breaking up the Boys' Club of Silicon Valley*. New York: Penguin.
- Chen, Janet X. and others, 2022. "Trauma-informed Computing: Towards Safer Technology Experiences for All." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–20.
- Chen, Mei and Michel Decary, 2020. "Artificial Intelligence in Healthcare: An Essential Guide for Health Leaders." *Healthcare Management Forum* 33(1): 10–18.
- Chetty, Krish and others, 2018. "Bridging the Digital Divide: Measuring Digital Literacy." *Economics* 12.
- Choi, Kyung-Shick and Hannarae Lee, 2023. "The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response." *Journal of Child Sexual Abuse* 16: 1–20.
- Christia, Fotini and others, 2021. "Violence against Women amid COVID-19: The Effects of Social and Traditional Media Campaigns to Empower Women: Pre-Analysis Plan." Website: fotini.mit.edu/sites/default/files/images/Egypt_PAP.pdf, accessed 3 April 2024.

- Costanza-Chock, Sasha, 2020. *Design Justice: Community-led Practices to Build the Worlds We Need*. Cambridge, MA: MIT Press.
- Cox, Joseph, 2022. "Data Broker SafeGraph Stops Selling Location Data of People Who Visit Planned Parenthood." *Motherboard*, 4 May. Website: www.vice.com/en/article/88gyn5/data-broker-safegraph-stops-selling-location-data-of-people-who-visit-planned-parenthood, accessed 3 April 2024.
- Crawford, Kate, 2022. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT: Yale University Press.
- D'Ignazio, Catherine and Lauren F. Klein, 2020. *Data Feminism*. Cambridge, MA: MIT Press.
- Dunn, Suzie and others, 2023. *Supporting Safer Digital Spaces*. Waterloo, ON: Centre for International Governance Innovation.
- Economist Intelligence Unit, 2021. "Measuring the Prevalence of Online Violence against Women." Website: onlineviolencewomen.eiu.com, accessed 3 April 2024.
- EHDS (The European Health Data Space), undated. "What Is the European Health Data Space?" Website: www.european-health-data-space.com, accessed 2 April 2024.
- eSafety Commissioner of Australia, 2018. "Understanding the Digital Behaviours of Older Australians: Summary of National Survey and Qualitative Research." Canberra: Office of the eSafety Commissioner.
- eSafety Commissioner of Australia, 2019. "Safety by Design Overview." Canberra: Office of the eSafety Commissioner.
- European Women's Lobby, 2017. *Her Net Her Rights: Mapping the State of Online Violence against Women and Girls in Europe*. Brussels: European Women's Lobby.
- Garçon, Loic, and others, 2016. "Medical and Assistive Health Technology: Meeting the Needs of Ageing Populations." *Gerontologist* Apr:56 Suppl 2:S293-302. Website: <https://pubmed.ncbi.nlm.nih.gov/26994268/>
- Gillett, Rosalie and others, 2022. "Safety for Whom? Investigating How Platforms Frame and Perform Safety and Harm Interventions." *Social Media + Society* 8(4).
- Gould, Helen A. F., 2022. "Fostering Trust in Technology: Focusing on Trust Relationships, Competency and Trust Mechanisms." Abstracts for the Governance of Emerging Technologies and Science Conference, May. Arizona State University School of Law. Website: events.asucollegeoflaw.com/wp-content/uploads/sites/44/2022/05/Gould-Trust.pdf, accessed 3 April 2024.
- GSMA, 2023. *The Mobile Gender Gap Report 2023*. London: GSMA.
- Gurumurthy, Anita, 2004. *Gender and ICTs*. Brighton, UK: Institute of Development Studies.
- Gurumurthy, Anita, 2006. "Promoting Gender Equality? Some Development-related Uses of ICTs by Women." *Development in Practice* 16(6): 611-616.
- Hafkin, Nancy J., 2006. *Cinderella or Cyberella? Empowering Women in the Knowledge Society*. Bloomfield, CT: Kumarian Press.
- Harris, Bridget A. and Delanie Woodlock, 2019. "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies." *British Journal of Criminology* 59(3): 530-550.
- Harris, Bridget A., and Delanie Woodlock, 2021. "For My Safety": Experiences of Technology-facilitated Abuse among Women with Intellectual Disability or Cognitive Disability." Melbourne: The eSafety Commissioner.

- Harris, Bridget and others, 2000. "Technology, Domestic Violence Advocacy and the Sustainable Development Goals." In *The Emerald Handbook of Crime, Justice and Sustainable Development*, Jarrett Blaustein and others (eds.), 295–314. Bingley, UK: Emerald Publishing Limited.
- Heger, Katharina and Christian P. Hoffmann, 2021. "Feminism! What Is It Good for? The Role of Feminism and Political Self-efficacy in Women's Online Political Participation." *Social Science Computer Review* 39(2).
- Helberger, Natali and others, 2018. "Governing Online Platforms: From Contested to Cooperative Responsibility." *The Information Society* 34(1): 1–14.
- Huang, Fei and others, 2017. "Beyond Pilotitis: Taking Digital Health Interventions to the National Level in China and Uganda." *Globalization and Health* 13(1).
- Hummel, Patrik and others, 2021. "Data Sovereignty: A Review." *Big Data & Society* 8(1): 1–17.
- Hussain, Hera, 2023. "Emergent Best Practices in Trauma-informed Design from Chayn's Interventions with and for Survivors of Technology Abuse." In *Technology and Domestic and Family Violence: Victimisation, Experiences and Responses*, Bridget Harris and Delanie Woodlock (eds), 192–198. London: Routledge.
- International Web Foundation, 2020. *IWF 2020 Annual Report: Face the Facts*. Washington DC: International Web Foundation.
- Internet Society and National Network to End Domestic Violence, undated. "Fact Sheet: Understanding Encryption – The Connections to Survivor Safety." Website: www.internetsociety.org/resources/doc/2020/understanding-encryption-the-connections-to-survivor-safety, accessed 3 April 2024.
- IPU (Inter-Parliamentary Union), 2016. "Sexism, Harassment and Violence against Women Parliamentarians." Issues Brief, October.
- ITU (International Telecommunication Union) and UN-OHRLS (United Nations Office of the High Representative for the Least Developed Countries, Landlocked Countries and Small Island Developing States), 2021. *Connectivity in the Least Developed Countries: Status Report 2021*. Geneva: ITU.
- ITU (International Telecommunications Union) and UNESCO (United Nations Educational, Scientific and Cultural Organization) Broadband Commission for Sustainable Development, 2022. *State of Broadband 2022: Accelerating Broadband for New Realities*. Geneva: ITU and UNESCO.
- Jellema, Anne and Ingrid Brudvig, 2015. *Women's Rights Online: Translating Access into Empowerment*. Washington, DC: World Wide Web Foundation.
- Kashyap, Ridhi and Emilio Zagheni, 2023. "Leveraging Digital and Computational Demography for Policy Insights." In *Handbook of Computational Social Science for Policy*, Eleonora Bertoni and others (eds.), 327–344. Cham, Switzerland: Springer.
- Kenyon, Miles, 2018. "Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System." The Citizen Lab, 26 September. Website: citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system, accessed 3 April 2024.
- Khoo, Cynthia, 2021. *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence*. Toronto, ON: Women's Legal Education and Action Fund.
- Kickbusch, Ilona and others, 2021. "The Lancet and Financial Times Commission on Governing Health Futures 2030: Growing up in a Digital World." *The Lancet* 398(10312): 1728.
- Latonero, Mark and Paula Kift, 2018. "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control." *Social Media + Society* 4(1).

- Leitão, Roxanne, 2019. "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse." *Proceedings of the 2019 Designing Interactive Systems Conference*, 527–539.
- Leong, Danielle, 2017. "Consensual Software: How to Prioritize User Safety." InfoQ, 18 May. Website: www.infoq.com/articles/consensual-software, accessed 3 April 2024.
- Lovett, Raymond and others, 2019. "Good Data Practices for Indigenous Data Sovereignty and Governance." In *Good Data*, Angela Daly and others (eds.), 26–36. Amsterdam: Theory on Demand.
- Ludwig, David and Phil Macnaghten, 2020. "Traditional Ecological Knowledge in Innovation Governance: A Framework for Responsible and Just Innovation." *Journal of Responsible Innovation* 7(1): 26–44.
- Mackey, April and Pammla Petrucka, 2021. "Technology as the Key to Women's Empowerment: A Scoping Review." *BMC Women's Health* 21, 78.
- McLachlan, Freya and Bridget Harris, 2022. "Intimate Risks: Examining Online and Offline Abuse, Homicide Flags, and Femicide." *Victims & Offenders* 17(5): 623–646.
- Macnaghten, Phil and others, 2014. "Responsible Innovation across Borders: Tensions, Paradoxes and Possibilities." *Journal of Responsible Innovation* 1(2): 191–199.
- Maher, Hamid and others, 2022. *AI Is Essential for Solving the Climate Crisis*. Boston, MA: Boston Consultancy Group.
- Maylik, Aliya and Afshan Amray, 2023. "Pakistan and Educast." 67th Commission on the Status of Women, United Nations, New York, 13 March. [not sure what this is – paper?]
- Mejias, Ulises A. and Nick Couldry, 2019. "Datafication." *Internet Policy Review* 8(4).
- Melhem, Samia and others, 2009. *Information and Communication Technologies for Women's Socioeconomic Empowerment*. Washington, DC: World Bank.
- Mihaila, Sorina, 2023. "Expert Calls for Reform of 'Exploitative' Digital Advertising Practices in Femtech." *Femtech World*, 14 November. Website: www.femtechworld.co.uk/news/researcher-calls-for-reform-of-exploitative-digital-advertising-in-femtech, accessed 3 April 2024.
- Ndjibu, Ruben and others, 2017. "Gender-based Violence Campaign in Namibia: Traditional Meets Technology for Societal Change." *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 127655: 1024–1029.
- NNEDV (National Network to End Domestic Violence) Safety Net Project, 2016. "Why Privacy and Confidentiality Matters for Victims of Domestic & Sexual Violence." Website: www.techsafety.org/privacymatters, accessed 3 April 2024.
- Núñez Puente, Sonia, 2011. "Feminist Cyberactivism: Violence against Women, Internet Politics, and Spanish Feminist Praxis Online." *Continuum* 25(3): 333–346.
- Nyst, Carly, 2014. *Technology-related Violence against Women: Recent Legislative Trends*. Association for Progressive Communications (APC).
- Oh, Sandra Soyeon and others, 2021. "Measurement of Digital Literacy among Older Adults: Systematic Review." *Journal of Medical Internet Research* 23(2).
- Owen, Richard and others, 2013. "A Framework for Responsible Innovation." In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, Richard Owen and others (eds.), 27–50. Chichester, UK: John Wiley & Sons.

- Parmentier, Mary Jane C. and Sophia Huyer, 2008. "Female Empowerment and Development in Latin America: Use versus Production of Information and Communications Technology." *Information Technologies & International Development* 4(3): 13–20.
- PenzeyMoog, Eva, 2020. *Design for Safety*. New York: A Book Apart.
- Perset, Karine, 2010. "The Economic and Social Role of Internet Intermediaries." OECD Digital Economy Papers No. 171. Paris: OECD Publishing.
- Pfitzner, Naomi and Jasmine McGowan, 2023. "Locked out or Let in? Learning from Victim-Survivors' Remote Help-seeking Experiences during COVID-19." *Journal of Gender-based Violence* 1–20.
- Plan International, 2020. *State of the World's Girls 2020: Free to Be Online? Girls' and Young Women's Experiences of Online Harassment*. Woking, UK: Plan International.
- Posetti, Julie and others, 2021. *The Chilling: Global Trends in Online Violence against Women Journalists*. New York: United Nations Children's Fund (UNICEF).
- Purdon, Lucy, 2023. *Unfinished Business: Incorporating a Gender Perspective into Digital Advertising Reform in the UK and EU*. San Francisco, CA: Mozilla Foundation.
- Ragnedda, Massimo, 2020. "Theorizing Inequalities." In *Enhancing Digital Equity: Connecting the Digital Underclass*, Massimo Ragnedda (ed), 11–37. Cham, Switzerland: Springer.
- Reconfigure Network, 2021. "Re:configure: Feminist Action Research in Cybersecurity." Website: www.oii.ox.ac.uk/wp-content/uploads/2021/01/Reconfigure-Report.pdf, accessed 3 April 2024.
- Richard, Gabriella T. and Kishonna L. Gray, 2018. "Gendered Play, Racialized Reality: Black Cyberfeminism, Inclusive Communities of Practice, and the Intersections of Learning, Socialization, and Resilience in Online Gaming." *Frontiers* 39(1), 112–148.
- Sadowski, Jathan, 2019. "When Data Is Capital: Datafication, Accumulation, and Extraction." *Big Data & Society* 6(1).
- Sareeta, Amrute, 2020. "Bored Technies Being Casually Racist: Race as Algorithm." *Science, Technology & Human Value* 45(5).
- Schorck, Nicholas J., 2019. "Artificial Intelligence and Personalized Medicine." *Cancer Treatment and Research* 178: 265–283.
- Schwalbe, Nina and Brian Wahl, 2020. "Artificial Intelligence and the Future of Global Health." *The Lancet* 395(10236): 1579–1586.
- Sharma, Chitragada and Akhila Kolisetty, undated. "Advancing Survivor-Centric, Intersectional Policy to Tackle Tech-facilitated Gender Based Violence." End Cyber Abuse. Website: endcyberabuse.org/advancing-survivor-centric-intersectional-policy-to-tackle-tech-facilitated-gender-based-violence, accessed 3 April 2024.
- Shirazi, Farid, 2012. "Information and Communication Technology and Women Empowerment in Iran." *Telematics and Informatics* 29(1): 45–55.
- Shroff, Geeta and Matthew Kam, 2011. "Towards a Design Model for Women's Empowerment in the Developing World." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2867–2876.
- Slakoff, Danielle C. and others, 2020. "The Role of Service Providers, Technology, and Mass

Media when Home Isn't Safe for Intimate Partner Violence Victims: Best Practices and Recommendations in the Era of COVID-19 and Beyond." *Archives of Sexual Behavior* 49: 2779–2788.

Slupska, Julia and Leonie Maria Tanczer, 2021. "Threat Modelling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things." In *The Emerald International Handbook of Technology-facilitated Violence and Abuse*, Jane Bailey and others (eds.), 663–688. Bingley, UK: Emerald Publishing Limited.

Slupska, Julia and others, 2021. "Cybersecurity Must Learn from and Support Advocates Tackling Online Gender-based Violence." UNIDIR, 12 August. Website: [unidir.org/cybersecurity-must-learn-from-and-support-advocates-tackling-online-gender-based-violence](https://www.unidir.org/cybersecurity-must-learn-from-and-support-advocates-tackling-online-gender-based-violence), accessed 3 April 2024.

Smith, Genevieve and Ishita Rustagi, 2021. "When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity." *Stanford Social Innovations Review*, 31 March.

Solid, undated. "Solid: Your Data, Your Choice." Website: solidproject.org, accessed 2 April 2024.

Stardust, Zahra and others, 2023. "Surveillance Does not Equal Safety: Police, Data and Consent on Dating Apps." *Crime, Media, Culture* 19(2).

Statista, undated. "Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2020, with Forecasts from 2021 to 2025." Website: www.statista.com/statistics/871513/worldwide-data-created, accessed 2 April 2024.

Stilgoe, J., Owen, R. & Macnaghten, P. op cit; [Is this Owen?]

Suzor, Nicolas P., 2019. *Lawless: The Secret Rules that Govern Our Digital Lives*. Cambridge, UK: Cambridge University Press.

Suzor, Nicolas P., and others, 2019. "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-based Violence Online." *Policy & Internet* 11(1): 84–103.

Sweeney, L., 2000. "Simple Demographics Often Identify People Uniquely." Data Privacy Working Paper 3. Carnegie Mellon University, Pittsburgh, PA.

Thakur, Dhanaraj and Asha Allen, 2022. "The Impacts of Online GBV and Disinformation on Women Politicians in Representative Democracies." Paper prepared for the Expert Group Meeting of the sixty-seventh session of the Commission on the Status of Women.

The Engine Room, 2023. Biometrics in the Humanitarian Sector: A Current Look at Risks, Benefits and Organisational Policies." Website: www.theengineerroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf, accessed 2 April 2024.

UN HRC (United Nations Human Rights Council), 2018. "Report of the Special Rapporteur on Violence Against Women, its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective." A/HRC/38/47.

UN OHCHR (United Nations Office of the High Commissioner for Human Rights), 2022. *Right to Privacy in the Digital Age*. New York: United Nations.

UN OHCHR (United Nations Office of the High Commissioner for Human Rights), 2020. "The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper." Website: www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf, accessed 3 April 2024.

- UN OHCHR (United Nations Office of the High Commissioner for Human Rights) and University of Essex, 2023. "Digital Border Governance: A Human Rights-based Approach." Website: www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf, accessed 3 April 2024.
- UNCTAD (United Nations Conference on Trade and Development), 2018. *Technology and Innovation Report 2018: Harnessing Frontier Technologies for Sustainable Development*. Geneva: United Nations.
- UNDESA (United Nations Department of Economic and Social Affairs), 2020. *Report of the UN Economist Network for the UN 75th Anniversary: Shaping the Trends of Our Time*. New York: United Nations.
- UNDESA (United Nations Department of Economic and Social Affairs), Statistics Division, 2105. *The World's Women 2015: Trends and Statistics*. New York: United Nations.
- UNDG (United Nations Development Group), 2017. *Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda*. New York: UNDG.
- UNECE (United Nations Economic Commission for Europe), 2021. "Ageing in the Digital Era." UNECE Policy Brief on Ageing No. 26. Website: https://unece.org/sites/default/files/2023-03/PB26-ECE-WG.1-38_E.pdf.
- UNFPA (United Nations Population Fund), 2012. *Ageing in the Twenty-First Century: A Celebration and a Challenge*. New York: UNFPA. Website: <https://www.unfpa.org/publications/ageing-twenty-first-century>.
- UNFPA (United Nations Population Fund), 2014. *International Conference on Population and Development: Programme of Action. 20th Anniversary Edition*. New York: United Nations.
- UNFPA (United Nations Population Fund), 2021. *Making all Spaces Safe: Technology-facilitated Gender-based Violence*. New York: UNFPA.
- UNFPA (United Nations Population Fund), 2022. *Preventing Technology-facilitated Gender-based Violence: Responding to the 2030 Agenda and "Our Common Agenda" by Proactively Mitigating Technology-facilitated Gender-based Violence by Enhancing Product Design, Data Privacy and Security, and Legal Frameworks to Hold Offenders Accountable*. New York: UNFPA.
- UNFPA (United Nations Population Fund), 2023. *Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices: Implementation Summary*. New York: UNFPA.
- UNICEF (United Nations Children's Fund) and ITU (International Telecommunication Union), 2020. *How Many Children and Young People have Internet Access at Home? Estimating Digital Connectivity During the COVID-19 Pandemic*. New York: UNICEF.
- United Nations, 1992. *United Nations Framework Convention on Climate Change*.
- United Nations, 2023. *Report on the 2022 Transforming Education Summit*. New York: United Nations.
- United Nations AI Advisory Board, 2023. "Interim Report: Governing AI for Humanity." Website: www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf, accessed 3 April 2024.
- Unwin, Tim, 2017. *Reclaiming Information and Communication Technologies for Development*. Oxford: Oxford University Press.

- Vasen, Federico, 2017. "Responsible Innovation in Developing Countries: An Enlarged Agenda." In *Responsible Innovation 3: A European Agenda?*, Lotte Asveld and others (eds.), 93-109. Cham, Switzerland: Springer.
- Wajcman, Judy, 2004. *TechnoFeminism*. Cambridge, UK: Polity Press.
- Wahl, Brian and others, 2019. "Artificial Intelligence (AI) and Global Health: How Can AI Contribute to Health in Resource-poor Settings?" *British Medical Journal Global Health* 3(4).
- Waldman, Linda and Marion Steven, 2015. *Sexual and Reproductive Health Rights and Information and Communications Technologies: A Policy Review and Case Study from South Africa*. Brighton, UK: Institute of Development Studies.
- West, Mark and others, 2019. *'I'd Blush if I Could': Closing Gender Divides in Digital Skills Through Education*. EQUALS and United Nations Educational, Scientific and Cultural Organization (UNESCO).
- WHO (World Health Organization) 2021a, *Global Strategy on Digital Health*. Geneva, WHO.
- WHO (World Health Organization), 2021b. *Violence against Women Prevalence Estimates, 2018: Global, Regional and National Prevalence Estimates for Intimate Partner Violence against Women and Global and Regional Prevalence Estimates for Non-partner Sexual Violence against Women. Executive Summary*. Geneva: WHO.
- Wilson Centre and UNFPA (United Nations Population Fund), 2023. *2022 Global Symposium on Technology-facilitated Gender-based Violence Results: Building a Common Pathway*. New York: UNFPA.
- Wilson, David and others, 2021. "Technology and Universal Health Coverage: Examining the Role of Digital Health." *Journal of Global Health* 11: 16006.
- Woodhouse, Teddy, 2021. *Affordability Report 2021*. Washington, DC: Alliance for Affordable Internet.
- World Bank, 2018. *Engendering ICT Toolkit*. Washington, DC: The World Bank.
- World Bank, 2021. *World Development Report 2021: Data for Better Lives*. Washington, DC: The World Bank.
- World Wide Web Foundation, 2020. *Women's Rights Online: Closing the Digital Gender Gap for a More Equal World*. Web Foundation. Website: webfoundation.org/docs/2020/10/Womens-Rights-Online-Report-1.pdf, accessed 3 April 2024.
- World Wide Web Foundation, 2021. *Tech Policy Design Lab: Online Gender-based Violence and Abuse. Outcomes and Recommendations*. Washington, DC: World Wide Web Foundation.
- Zarnowiecki, Dorothy and others, 2019. *Digital Platforms as Effective Health Promotion Tools: An Evidence Check Review*. Sydney: Sax Institute.
- Zeiter, Kirsten and others, 2019. *Tweets that Chill Report: Analyzing Online Violence against Women in Politics*. Washington, DC: National Democratic Institute.
- ZICTA (Zambia Information and Communications Technology Authority), 2023. *Online Gender-based Violence Among Women and Girls in Zambia: An Assessment of the Nature, Extent and Effects of Online Gender-based Violence among Women and Girls in Zambia*. Lusaka: ZICTA.
- Zweig, Janine M. and others, 2013. *Technology, Teen Dating Violence and Abuse, and Bullying*. Washington, DC: Urban Institute.

Endnotes

- 1 Digital public infrastructure is a comprehensive system of digital services, tools and technologies provided by governments, organizations and other stakeholders to facilitate the functioning of a digital society.
- 2 UNCTAD 2018.
- 3 Dunn and others 2023; Melhem and others 2009.
- 4 World Wide Web Foundation 2020.
- 5 Owen and others 2013.
- 6 Benjamin 2019.
- 7 UNFPA 2022.
- 8 Khoo 2021, p. 3.
- 9 European Women's Lobby 2017.
- 10 UNFPA 2021, p. 25; McLachlan and Harris 2022.
- 11 The Institut Public de Sondage d'Opinion Secteur contends that 41 per cent of French people have been targeted at least once by online violence, but this number rises to 85 per cent for French women under 35.
- 12 Economist Intelligence Unit 2021; Thakur and Allen 2022.
- 13 Alencar 2023; Kenyon 2018; Latonero and Kift 2018.
- 14 Economist Intelligence Unit 2021; Posetti and others 2021; Zeiter and others 2019.
- 15 Jellema and Brudvig 2015; Perset 2010; UNDESA 2020.
- 16 Borges do Nascimento and others 2022.
- 17 While approximately two thirds of the world's population lives in countries with below-replacement fertility (2.1 births per woman), more than 30 countries or areas have fertility levels above 4 births per woman. And while the pace of population ageing varies widely among countries, the proportion of people aged 60 and older currently makes up 12.3 per cent of the global population. By 2050, the share will rise to almost 22 per cent.
- 18 Kashyap and Zagheni 2023.
- 19 This term refers to the processes of digitalization, which include changes to associated processes such as the digitization of survey forms and methods for assessing survey results.
- 20 There is no universally agreed international definition of youth as an age group. For statistical purposes, the United Nations, without prejudice to any other definitions made by Member States, defines "youth" as those persons between the ages of 15 and 24 years.
- 21 Perez, Cohen-Jarvie and Drew. 2021; Melhem and others 2009.
- 22 United Nations 2023.
- 23 Ibid.
- 24 Anderson and Jiang 2018.
- 25 International Web Foundation 2020.
- 26 Zweig and others 2013.
- 27 Center for Countering Digital Hate 2022.
- 28 Plan International 2020.
- 29 Jellema and Brudvig 2015; Perset 2010; UNDESA 2020.
- 30 An example is the work of Educast, which provides education and e-health career pathways for women doctors in Afghanistan, Canada, China, Oman, Pakistan, Saudi Arabia, the State of Palestine, the United States of America and Yemen, as discussed at the United Nations at the sixty-seventh Commission on the Status of Women. See Maylik and Amray 2023.
- 31 See, for instance, Aceng 2023. Other examples include the cyberharassment helpline in Pakistan administered by the Digital Rights Foundation.
- 32 Chen and Decary 2020; Mackey and Petrucka 2021; Schwalbe and Wahl 2020; WHO 2021a.
- 33 Harris and others 2020; Wahl and others 2019.
- 34 Harris and others 2020.
- 35 Christia and others 2021; Gurumurthy 2006; Waldman and Steven 2015; Wilson and others 2021; WHO 2021a; Zarnowiecki and others 2019.
- 36 Harris and others 2020; Pfitzner and McGowan 2023; Slakoff and others 2020.
- 37 Schork 2019.
- 38 Huang and others 2017; Mackey and Petrucka 2021; UNDESA 2020; Waldman and Stevens 2015.
- 39 UNDESA 2020; WHO 2021a.
- 40 Abdenur and Brasil 2019.
- 41 UN OHCHR and University of Essex 2023.
- 42 United Nations 1992, articles 4(1), 4(5).

- 43 Maher and others 2022.
- 44 Bernal Aparicio and Siope Vakataki 2021.
- 45 Alaoui 2015.
- 46 APC 2018; Ceia and others 2021; Hafkin 2006; Dunn and others 2023; Heger and Hoffmann 2021; Melhem and others 2009; Nuñez Puente 2011; Shirazi 2012.
- 47 UN OHCHR 2020.
- 48 Richard and Gray 2018.
- 49 See eSafety Commissioner of Australia 2019 and associated resources, which can be accessed at: <https://www.esafety.gov.au/industry/safety-by-design>.
- 50 An end-user is a person who makes use of the tech product. An end-user may differ from a customer, since the entity or person that buys a product or service may not be the one who actually uses it.
- 51 Hussain 2023; Melham and others 2009; Parmentier and Huyer 2008. See also: TermsWeServeWith.Org.
- 52 Chen and others 2022.
- 53 Reconfigure Network 2021; Leitão 2019; Caravan Studios 2024.
- 54 Owen and others 2013; Costanza-Chock 2020.
- 55 Macnaghten and others 2014; Vasen 2017; Ndjibu and others 2017; Ludwig and Macnaghten 2020.
- 56 Slupska and Tanczer 2021.
- 57 WHO 2021b.
- 58 Harris and others 2000; Pfitzner and others 2023.
- 59 Gillett and others 2022; Stardust and others 2023.
- 60 Harris and Woodlock 2019.
- 61 eSafety Commissioner of Australia 2019; Harris and Woodlock 2021; Hussain 2023; Leong 2017; Sharma and Kolisetty, undated.
- 62 Andere and Kathure 2023.
- 63 Slupska and others 2021.
- 64 Crawford 2022.
- 65 Dunn and others 2023; Harris and Vitis 2020; PenzeyMoog 2020; Suzor and others 2019; Suzor 2019.
- 66 Smith and Rustagi 2021.
- 67 Chang 2019; Gurumurthy 2004; Harris and Vitis 2020; Marcelle 2017; Ragnedda 2020; Sareeta 2020; Wajcman 2004.
- 68 Ceia and others 2021; Chetty and others 2018; Ragnedda 2020; Unwin 2017.
- 69 GSMA 2023.
- 70 Adegoke 2022; Chair and De Lannoy 2018; ITU and UN-OHRLS 2021; ITU and UNESCO 2022; UNICEF and ITU 2020.
- 71 Carlson 2006; eSafety Commissioner of Australia 2018; Garçon and others 2016; UNDESA 2020; UNECE 2021; UNFPA 2012.
- 72 Broadband Commission Working Group on Broadband and Gender 2013; UNDESA 2020; Jellema and Brudvig 2015.
- 73 Alliance for Affordable Internet 2020.
- 74 Broadband Commission Working Group on Broadband and Gender 2013; Woodhouse 2021; World Bank 2018.
- 75 Broadband Commission Working Group on Broadband and Gender 2013; UNDESA 2020; UNDESA, Statistics Division 2015; Jellema and Brudvig 2015.
- 76 Harris and Woodlock 2021.
- 77 UNDESA 2020; Jellema and Brudvig 2015.
- 78 GSMA 2023, see also Auxier and others 2020; Choi and Lee 2023.
- 79 Chetty and others 2018; Perset 2010; Jellema and Brudvig 2015; West and others 2019.
- 80 TF GBV is an umbrella term that incorporates a range of harms, enacted by a variety of actors, and in many contexts, settings and dynamics. It is 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 technologies against a person on the basis of their gender. It may be perpetrated by individuals, networks, communities, corporations and States. It is an easy and cheap way to perpetrate and propagate violence against individuals or a group of people in the case of disinformation campaigns. UNFPA 2022.
- 81 ZICTA 2023; Anwar and others 2023.
- 82 Posetti and others 2021.
- 83 IPU 2016.
- 84 Pfitzner and others 2023; UNDESA 2020; Jellema and Brudvig 2015.
- 85 UN OHCHR 2020.
- 86 Suzor and others 2019.
- 87 See: "Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025" at Statista, undated.
- 88 Slupska and Tanczer 2021.

- 89 Sadowski 2019; Mejias and Couldry 2019.
- 90 The Engine Room 2023.
- 91 Purdon 2023, p. 4; see also Mihaila 2023.
- 92 Purdon 2023.
- 93 Personal correspondence with Laura Bates.
- 94 Cox 2022. The move comes after Motherboard found it was possible to buy data showing how many people visited Planned Parenthood.
- 95 Centre for Humdata 2020.
- 96 Sweeney 2000.
- 97 Solid, undated.
- 98 Cavoukian 2011.
- 99 D'Ignazio and Klein 2020.
- 100 As in the context of the European Health Data Space, see EDHS, undated. This approach is being rolled out by the Flemish Data Utility Company (Atoumi).
- 101 Hummel and others 2021.
- 102 Wilson and others 2021.
- 103 NNEDV Safety Net Project 2016.
- 104 Internet Society and National Network to End Domestic Violence, undated.
- 105 United Nations AI Advisory Board 2023.
- 106 Kickbusch and others 2021, p. 1728.
- 107 Ibid.
- 108 Ceia and others 2021; Ceia, Nothwehr and Wagner, 2021; Dunn and others 2023; UNDG 2017; UN HRC 2022; Wilson Centre and UNFPA 2023.
- 109 UN OHCHR 2020.
- 110 Shroff and Kam 2011.
- 111 World Wide Web Foundation 2021.
- 112 UNFPA 2023.
- 113 eSafety Commissioner of Australia 2019.
- 114 Gould 2022.
- 115 Athar 2015; Nyst 2014; Perset 2010; Suzor and others 2019.
- 116 Ibid.
- 117 Specifically, proactive measures within technology products, including: (1) visible, easily accessible, plain-language complaint and abuse reporting mechanisms on harmful content, including in end-user local languages; (2) effective internal triaging and escalation of complaints; (3) effective internal protocols for connecting with law enforcement and support services and hotlines for illegal content; (4) establishment of internal teams responsible for implementing user safety policies; (5) improved user consent through social contracts between users, services and third parties at the time of registration; (6) training of all staff to understand their role in monitoring and removal of harmful content relating to TF GBV; and (7) provision of independent audits and the publication of comprehensive annual transparency reports, including gender-disaggregated data, relating to implementation of the policies.
- 118 Helberger and others 2018; UNHRC 2018; UNFPA 2023.



United Nations Population Fund
605 Third Avenue
New York, NY 10158
Tel. +1 212-297-5000
www.unfpa.org
X@UNFPA

