Transforming Digital Landscapes in South Asia: Empowering Changemakers for Inclusive Tech

Capacity Building Toolkit

CUTS International 1983-2023

#2514

Transforming Digital Landscapes in South Asia: Empowering Changemakers for Inclusive Tech

Capacity Building Toolkit

Published by

CUTS International
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Authors:
Krishaank Jugiani, *Senior Research Associate, CUTS International*
Asheef Iqubbal, *Senior Research Associate, CUTS International*
Bijaya Roy, *Senior Research Associate, CUTS International*
Samridh Shastry, *Policy Analyst, CUTS International*
Deepmala Ghosh, *Research Associate, CUTS International*
Sobhan Guha, *Programme Associate, CUTS International*

#2514

Contents

Acknowledgement

This module is the result of collective efforts and thoughtful contributions from our colleagues at CUTS International. This module serves as a foundational guide, providing essential concepts and strategies. It is not intended as an advanced training resource but rather as a starting point for further learning and engagement.

We extend our gratitude to Amol Kulkarni, Director (Research) at CUTS International, for his constant guidance, thought-provoking discussions, and leadership throughout this project.

We also deeply appreciate the review and feedback provided by Shivangi Tyagi (former consultant, CUTS International), which helped refine and strengthen the module. The module also benefited from the dedicated support of our colleagues: Akshay Sharma, Senior Programme Officer, Atul Sharma, Assistant Policy Analyst and Shivani Ilangovan, Research Associate.

The Publications Team at CUTS International- Madhuri Vasnani, Shivendra Shekhawat, and Mukesh Tyagi- deserve special recognition for their exceptional effort in bringing this module to fruition.

We acknowledge the contributions of several other individuals who, while not named here, played crucial roles in the success of this project.

Any errors or omissions that remain are solely our responsibility.

Background and Context

Digital transformation is advancing in South Asia, with governments adopting new laws, policies, and approaches to utilise and develop digital technologies that impact the social and economic well-being of citizens. However, some proposed and existing regulations can have a negative impact on women and youth, such as violation of privacy, online censorship and internet shutdowns, restricting access to information during elections and protests. These unforeseen consequences disproportionately affect women and young people, depriving them of an avenue for challenging entrenched social norms and power dynamics. To promote technologies that uphold democratic values, it is crucial to ensure the active involvement of women and youth in shaping internet governance and digital policies. In this context, through the '***Protecting Rights of Online Changemakers' (PORCH)*** initiative, CUTS in partnership with Internews and other organisations in Bangladesh, India, Nepal, and Sri Lanka, aims to facilitate the centring of the voices of youth and women in digital policymaking in these countries.

Objective

PORCH has adopted a multi-pronged approach to create a positive impact on women and youth. To achieve the project's goals, we have created a course intended for workshops that build the capacity of women and youth to engage actively in the digital policymaking space. This course aims to equip groups working with women and youth in South Asia with the necessary skills and knowledge and strengthen their capacity on issues related to digital rights and relevant national and international laws. The objective is to support them in developing sustainable localised advocacy campaigns, actively engage with relevant stakeholders and build a safe and transparent digital space. This includes women and youth-led organisations, content creators, Human Rights Defenders, and journalists, among others. Subsequently, through workshops based on the course, we aim to facilitate interactions between targeted groups, developing a collaborative approach to shape policies that not only facilitate technological innovation but also uphold principles of accountability and rights-respecting practices.

Major Laws Governing Digital Spaces

Samridh Shastry
Policy Analyst

Welcome to the exciting world of digital laws! In this first module, we will embark on a journey through the legal and regulatory landscape that shapes our interactions in the online world. As technology evolves rapidly, understanding the laws governing our digital lives is essential for protecting our rights. We'll explore broad principles and key thematic areas that will provide you with a solid foundation to navigate the complexities of digital laws.

Introduction

Learning Objectives

Digital rights are more than just legal jargon — they help ensure a fair and empowering online experience. In this chapter, we'll explore how digital rights are essentially an extension of fundamental human rights into the digital realm. Our learning objectives are to help you understand the core principles of digital rights, recognise how these rights protect individuals in online spaces, and develop a critical lens for examining digital laws. We'll break down complex concepts into digestible insights, focusing on how these rights specifically impact women, youth, and marginalised communities in South Asian contexts. By the end of this module, you'll be equipped to identify, understand, and advocate for digital rights that protect individual freedoms, ensure online safety, and promote equitable digital participation.

What are Digital Rights?

To kick things off, let's delve into the concept of digital rights. These rights are recognised as fundamental human rights in the online realm, mirroring those outlined in the United Nations' Universal Declaration of Human Rights (UDHR).[1] They include, but are not limited to, crucial elements such as the right to privacy, freedom of expression, and access to information. Imagine a world where everyone has equal access to the internet; where your voice can be heard without fear of censorship; where

[1] https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/

your personal data is safeguarded against unauthorised access. This is the essence of digital rights.

Why digital rights matter for women, youth, and minorities

In the vast landscape of the digital world, vulnerabilities can quickly transform into dangers. For women, youth, and minority groups, digital rights are not just theoretical concepts, they are lifelines of protection and empowerment. These groups often face disproportionate risks online,[2] including cyberbullying, harassment, privacy breaches, and systemic exclusion.[3] Digital rights serve as a critical shield, ensuring that these individuals can access information, express themselves freely, maintain personal privacy, and participate meaningfully in digital spaces without fear of discrimination or violence. In the context of South Asian countries like India, Nepal, Bangladesh, and Sri Lanka, where social hierarchies and digital divides intersect, understanding and claiming digital rights becomes a powerful tool for social transformation and individual agency. Since women and youth users are more vulnerable than others, they have to overcome social barriers to navigate the digital space, and typically have limited social and economic freedom.[4]

As we unpack this topic, we will highlight key digital rights that feature in jurisdictions around the world, such as access to the internet, freedom of speech and expression, privacy protections, the right to be forgotten, and digital security. It is important to remember that most digital rights are derived from general human rights - digital rights are, in essence, human rights in the digital age.[5] By understanding these dynamics, we can better appreciate how laws can empower or disempower individuals in their online interactions.

How to analyse laws critically

Critically analysing laws is like being a detective. You're not just reading the text, but unpacking its deeper meanings, potential impacts, and hidden implications. Start by asking key questions: Whose interests does this law truly serve? Who might be marginalised or left unprotected? Look beyond the surface-level language and examine the practical consequences of legal provisions. Consider the context of

2 https://www.unwomen.org/en/news-stories/op-ed/2023/05/op-ed-digital-rights-are-womens-rights

3 https://equalitynow.org/news_and_insights/young-people-and-digital-rights-perspectives-from-southern-africa/

4 Statement: From clicks to progress – Equality in digital access advances rights for young women and girls | UN Women – Headquarters

5 Human rights in the digital age | OHCHR

implementation — how might a law play out in real-world scenarios, especially for vulnerable populations? Pay attention to gaps, ambiguities, and potential loopholes that could be exploited. Compare the law with international human rights standards and examine whether it genuinely protects individual freedoms or inadvertently creates new forms of control. Remember, a law's true strength lies not in its words, but in its ability to create fair, inclusive, and just digital environments for all.

Understanding Digital Rights in Practice

Rights framework

1. **Access to the Internet** isn't just about having a smartphone or Wi-Fi — it's your gateway to a world of opportunities. This fundamental right is about ensuring everyone, regardless of their background, can meaningfully participate in our digital world. Think about a young student in a remote village being able to access online classes, or a woman entrepreneur reaching customers through social media. This right has been recognised by courts in several South Asian countries as essential for modern life, making it harder for authorities to impose arbitrary restrictions or shutdowns.

2. The **Right to Information** is in your hands. It's your tool to ask questions, verify facts, and hold institutions accountable in the digital age. It empowers you to check if your personal data is being properly protected, or to understand how government decisions affecting your online life are made. This right goes beyond just accessing information — it's about being able to understand it, use it, and share it effectively. For example, you can use this right to find out how your data is being used by government agencies or why certain websites are blocked in your region.

3. **Freedom of Speech and Expression** ensures that your voice matters. Whether you're sharing your thoughts on social media, creating content, or participating in online discussions, this freedom is essential for democratic participation. However, in South Asian contexts, we often see governments using broad terms like 'national security' or 'public order' to restrict online expression. Understanding these limitations helps you navigate the boundaries between protected speech and potential restrictions, allowing you to express yourself while protecting your rights.

4. **The right to Privacy and Data Protection** is imperative in our increasingly data-driven world. In an era where our lives are increasingly online, privacy isn't just about keeping secrets — it's about having control over your personal information. This right ensures you can decide how your data is collected, used, and shared. Whether it's protecting your social media activity from surveillance, securing your financial transactions, or maintaining confidentiality in your online communications, privacy rights are crucial for having autonomy and dignity in the digital world.

5. **Digital Security** rights protect you from various threats in cyberspace, from hacking to identity theft. These rights are particularly crucial for vulnerable groups like women and young people, who often face targeted online threats. Good digital security means not just using strong passwords, but also having systems, laws, and practices that protect your digital life. This includes the right to use encryption, secure communication tools, and other protective measures without unnecessary interference.

This framework sets the stage for understanding how these rights play out in real situations (which we'll explore in the following sections), how they're often violated, and most importantly, how people like you have successfully defended them. Each right connects with the others, creating a web of protections that, when properly implemented, helps ensure a safer, more inclusive digital world for everyone.

Real-world applications

Let's bring these digital rights to life through everyday scenarios. Consider a young woman in rural Bangladesh using her smartphone to access online education — this is the right to internet access in action. Or think about a youth-led organisation in Nepal using social media to raise awareness about environmental issues — that's freedom of expression at work. Digital rights shape our daily experiences in countless ways: when you decline unnecessary cookie permissions on a website (privacy rights), when you verify news through fact-checking websites (right to information), or when you use two-factor authentication for your email (digital security). These rights aren't just abstract concepts; they're practical tools that protect and empower you every time you go online, whether you're shopping, studying, socialising, or seeking important information about government services.

Common violations

Understanding how digital rights can be violated helps us recognise and respond to threats more effectively. Some common violations include:

1. Internet shutdowns during protests or examinations
2. Social media surveillance and monitoring
3. Data breaches exposing personal information
4. Cyber harassment and online gender-based violence
5. Blocking of websites without transparent reasons
6. Mandatory sharing of personal data for basic services
7. Discriminatory content moderation
8. Digital exclusion of marginalised communities

These violations often disproportionately affect women, young people, and minority groups. For instance, women face higher rates of online harassment and privacy violations, while young people might encounter restrictions on accessing educational content due to broad filtering systems.

Case studies of rights defence

Let's look at inspiring examples of individuals and communities defending their digital rights:

1. *Internet Shutdowns in India*: In 2020, students and activists in India challenged prolonged internet shutdowns in Kashmir through legal action,[6] highlighting how citizens can use courts to protect their right to internet access.
2. *Internet Freedom Advocacy in Nepal*: In 2020, Nepali citizens, particularly youth and civil society organisations, mobilised against the proposed Information Technology Bill.[7] This bill contained severe restrictions on social media use and gave broad powers to authorities to block social media platforms without adequate safeguards. Through coordinated protests, public awareness campaigns, and strategic advocacy, they highlighted how the bill threatened freedom of expression online. Organisations like Body & Data led initiatives to raise awareness about privacy rights and data protection, particularly focusing on women's experiences in digital spaces.[8]

---

6 Anuradha Bhasin v. Union of India (2020) 3 SCC 637

7 https://kathmandupost.com/national/2020/01/11/organisations-gear-up-for-protest-against-it-bill-saying-it-will-curb-freedom-of-expression

8 https://bodyanddata.org/wp-content/uploads/2021/09/Policy-Paper_IT-Bill_Final-compressed.pdf

3. *Challenging Digital Controls in Bangladesh*: The movement against Section 57 of the ICT Act and later the Digital Security Act and the Cyber Security Act demonstrates the power of collective action. Civil society organisations, journalists, and human rights defenders consistently documented how these laws were being used to restrict online expression.[9] These efforts have helped build public awareness about digital rights and the importance of protecting free expression online.[10]
4. *Digital Rights during Crisis in Sri Lanka*: During the 2019 Easter attacks, when social media platforms were blocked,[11] NGOs documented the impact of internet shutdowns on citizens' rights and livelihoods. Organisations focused on digital literacy and safety, particularly that of vulnerable groups.[12] Their work shows how internet shutdowns can lead to misinformation and backlash,[13] especially during crises when these rights face the greatest threats.

These cases demonstrate that defending digital rights isn't just for lawyers or tech experts—it's for everyone! They show how understanding your rights, organising with others, and taking strategic action can create real change in the digital world.

Each case study reveals important lessons:

- Know your rights and the laws that protect them
- Document violations systematically
- Build networks and collaborate with others
- Use existing legal and advocacy tools
- Share successes to inspire and educate others

Legal Frameworks in Action

Law overview

In this chapter, we'll explore the laws governing digital rights. These laws aim to do two important things: protect users like you while making sure everyone has fair access

9 https://carnegieendowment.org/research/2021/12/how-bangladeshs-digital-security-act-is-creating-a-culture-of-fear?lang=en

10 https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act

11 https://www.nbcnews.com/tech/tech-news/sri-lanka-blocks-social-media-after-easter-sunday-bombings-n996886

12 https://gnet-research.org/2023/09/29/unmasking-islamophobic-disinformation-in-the-aftermath-of-sri-lankas-easter-sunday-attack/

13 https://www.usip.org/publications/2021/04/two-years-after-easter-attacks-sri-lankas-muslims-face-backlash

to technology. However, there's a challenging reality we need to understand - governments are increasingly putting restrictions on internet freedoms, often citing national security concerns. As of 2022, at least 53 countries had placed restrictions on online expression.[14] The COVID-19 pandemic highlighted just how important it is to have inclusive laws that address digital inequalities, as more of our daily lives moved online.[15]

Country-specific frameworks

1. **India's** digital legal journey started with the Information Technology Act of 2000, but it's evolved significantly since then. The biggest recent change is the Digital Personal Data Protection (DPDP) Act, 2023, which focuses on protecting your personal information. A key development was when India's Supreme Court declared internet access a fundamental right in 2020.[16] However, India also leads globally in internet shutdowns, particularly in regions like Jammu and Kashmir.[17] The government maintains significant control through the Information Technology Rules, 2021, which require social media platforms to assist in investigations and remove certain content.

Key Features of DPDP Act, 2023:[18]

- Requires explicit consent for using personal data
- Gives you rights to access, correct, and erase your data
- Allows you to transfer your data between services
- Can impose fines up to ₹250 crore for violation

2. **Bangladesh's** digital laws centre around the Cybersecurity Act, which followed the Digital Security Act of 2018, which had replaced the earlier ICT Act. The country's "Digital Bangladesh" vision[19] has increased internet access but also brought more surveillance. This digital transformation has been accompanied by increased surveillance capabilities and strict content monitoring systems. The government maintains strong oversight of social media platforms, and during

14 https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet
15 https://news.un.org/en/story/2021/06/1093422
16 *Anuradha Bhasin* v. *Union of India* (2020) 3 SCC 637
17 https://www.thehindu.com/sci-tech/technology/india-records-highest-number-of-internet-shutdowns-globally-in-2023/article68178061.ece
18 https://www.expresscomputer.in/news/examining-penalties-under-the-dpdp-act-2023/110701/
19 https://www.thedailystar.net/opinion/views/news/digital-bangladesh-story-transformation-resilience-and-sustainability-3222626

times of political unrest or protests, internet access has occasionally been restricted. The Information and Communication Technology Act was a powerful tool for the State, and lives on through the erstwhile Section 57 in provisions of the Cybersecurity Act.

These provisions give authorities broad powers to regulate online content and conduct investigations:

- Addresses content that could affect law and order
- Can result in up to 14 years imprisonment and fines up to Tk. 1 crore
- Gives broad powers to law enforcement for investigations

3. **Sri Lanka's** approach to digital governance has been shaped by its unique experiences with social media-driven unrest and security challenges. The foundation of its digital framework rests on the Computer Crimes Act of 2007 and the Electronic Transactions Act, but recent events have led to significant developments. The country's experience with social media-fueled unrest, particularly during the 2019 Easter bombings and the 2022 economic crisis, has influenced its regulatory approach. This has led to the introduction of the Online Safety Act, a highly controversial legislation[20] that includes plans for digital IDs and content monitoring systems. While Sri Lanka boasts relatively high internet penetration for the region, there's an ongoing tension between digital access and security concerns,[21] particularly regarding surveillance and the use of emergency powers to restrict online access.[22]

The Online Safety Act creates:

- An Online Safety Commission to regulate online content
- Rules against cyberbullying and false information
- Registration requirements for social media platforms
- Mechanisms for content removal, requiring platforms to act within specific timeframes when notified of violations

4. **Nepal's** approach to digital governance represents a unique balance in South Asia, with its framework primarily anchored by the Electronic Transaction Act 2063 (2008) and subsequent developments through the Information

20 https://www.bbc.com/news/world-asia-68163414
21 https://ohrh.law.ox.ac.uk/gendered-dimensions-a-critical-look-at-the-online-safety-act-of-sri-lanka/
22 https://www.amnesty.org/en/latest/news/2024/01/sri-lanka-online-safety-act-major-blow-to-freedom-of-expression/

Technology Bill. While the country's constitution explicitly guarantees freedom of expression, including digital rights, recent years have seen evolving approaches to digital governance. The government has been working to expand its regulatory framework, notably through the controversial Online Media Operation Directive. Compared to its South Asian neighbours, Nepal has historically maintained a less restrictive approach to internet governance, though recent years have witnessed increased efforts to regulate social media and online content. The National Information and Communication Technology Policy has played a crucial role in shaping the country's digital landscape, emphasising infrastructure development and digital literacy while addressing emerging cybersecurity concerns.

- The National Information and Communication Technology Policy establishes important guidelines for digital governance.
- The policy emphasises infrastructure development and digital literacy while addressing cybersecurity concerns.
- It sets frameworks for data protection, though these are generally less prescriptive than those found in other South Asian nations.

Stated objectives of digital laws

The overarching goals of these laws can be summarised in five key areas: protecting individual freedoms, ensuring equal access and preventing discrimination, safeguarding personal data and privacy, promoting transparency and accountability of platforms, and combating cybercrime and online harassment.

1. **Protecting individual freedoms** is at the heart of digital rights legislation. These laws are designed to ensure that individuals can express themselves freely online without fear of censorship or retaliation. This protection is vital for fostering a vibrant digital public sphere where diverse voices can be heard and where citizens can engage in meaningful dialogue about issues that matter to them. By safeguarding these freedoms, laws empower individuals to participate actively in society, advocate for their rights, and hold those in power accountable.
2. Another crucial objective is **ensuring equal access and preventing discrimination** in the digital realm. Access to the internet should not be a privilege reserved for a select few; rather, it should be a right enjoyed by all, regardless of socio-economic status, gender, or geographical location. Laws

that promote equal access help bridge the digital divide, ensuring that marginalised communities can benefit from the opportunities the internet offers. By preventing discrimination in accessing digital services and technologies, these laws work towards creating an inclusive online environment where everyone can thrive.

3. **Safeguarding personal data and privacy** is increasingly critical as our lives become more intertwined with technology. Digital rights laws aim to protect individuals' personal information from unauthorised access and misuse. This includes establishing clear guidelines on how data should be collected, stored, and shared by organisations. When individuals feel confident that their data is secure, they are more likely to engage with digital platforms and services. Privacy protections foster trust in technology and encourage users to explore the vast resources available online without fear of exploitation.
4. Moreover, promoting **transparency and accountability of platforms** is essential for maintaining a fair digital ecosystem. Laws that require companies to disclose how they collect and use data empower users to make informed choices about their online interactions. Transparency helps build trust between users and service providers while holding companies accountable for their practices. When platforms are required to operate with integrity, it leads to better protection of user rights and fosters a culture of responsibility within the tech industry.
5. Lastly, combating **cybercrime and online harassment** is a pressing objective of digital rights legislation. As our reliance on technology grows, so do the threats posed by malicious actors seeking to exploit vulnerabilities for personal gain or to harm others. Laws aimed at addressing cybercrime provide essential protections against activities such as hacking, identity theft, and online harassment. By creating legal frameworks that penalise such behaviours, these laws not only protect individuals but also promote a safer online environment where everyone can interact without fear of harm.

The reality of digital law enforcement

As we navigate the complex landscape of digital rights, it’s important to recognise the on-ground realities of how they are enforced. Despite the laws and regulations designed to protect these rights, various obstacles hinder their effective implementation and enforcement. These challenges include the regulation of online speech, varying degrees of digital surveillance, censorship, and the ongoing struggle against cybercrime and online harassment.

1. In the South Asian context, we observe various degrees of **digital surveillance** that pose significant threats to privacy and freedom of expression. Governments often justify surveillance measures as necessary for national security or public safety; however, such practices can lead to a chilling effect on free speech and discourage individuals from expressing dissenting opinions or engaging in open discussions online.
2. Moreover, the **proliferation of cybercrime**—including identity theft, hacking, and online harassment—further complicates the landscape. As more people engage with digital platforms, incidents of bullying and hate speech have surged, necessitating robust legal frameworks that not only address these issues but also protect victims effectively.
3. Another critical challenge is the **digital divide**, which exacerbates inequalities in access to technology. Rural populations often find themselves at a disadvantage due to inadequate infrastructure and resources, limiting their ability to participate fully in the digital economy. This divide highlights the urgent need for laws that ensure equal access to technology and prevent discrimination based on geographic or socio-economic factors.
4. The vast amounts of **personal data collected** by digital platforms also raise significant concerns regarding privacy protections. With increasing reliance on data-driven technologies, stronger data protection laws are essential to safeguard individuals' information from misuse or exploitation. The introduction of mandatory digital identification systems—like India's Aadhaar—has sparked debates about privacy implications and potential misuse in linking personal data with financial institutions or government services.
5. Additionally, **internet shutdowns** have become a tool for governments during times of civil unrest or political dissent. These shutdowns not only disrupt communication but also infringe upon individuals' rights to information and expression. As we examine country-specific case studies throughout this module, we will explore how laws can both empower and disempower vulnerable groups online. By understanding these challenges in depth, we can better advocate for policies that protect digital rights while promoting an inclusive digital future for all.

Implementational challenges

The path from written law to real-world protection isn't always smooth. Courts across South Asia are still working to interpret and apply these new digital laws effectively.

Take India's DPDP Act, for example – while it promises strong protections, its implementation has been slow, and experts are questioning whether it really balances citizen privacy with digital economic needs. In Bangladesh, the broad powers granted by the Cybersecurity Act have raised concerns about potential misuse, while Sri Lanka's courts are just beginning to address challenges under their new Online Safety Act.

The struggle to balance privacy with security creates another significant hurdle. Governments often justify increased surveillance and monitoring as necessary for national security, but these measures can silence free expression and discourage open online discussions. Internet shutdowns have become increasingly common during times of unrest, cutting off essential communication and access to information when it's most needed. The introduction of digital ID systems, while potentially beneficial for government services, raises serious questions about privacy and data protection.

Perhaps most concerning is the persistent digital divide that affects millions across South Asia. Rural communities often find themselves cut off from the digital world due to poor infrastructure and limited resources. This isn't just about having an internet connection – it's about having the knowledge, tools, and confidence to participate fully in digital spaces. When some communities lack access to these resources, they miss out on educational opportunities, economic advancement, and the chance to have their voices heard in increasingly important online discussions.

Impact on marginalised groups

The impact of digital rights legislation on marginalised groups—particularly women and youth—is profound yet often overlooked. In South Asia, these demographics frequently face heightened vulnerabilities online due to systemic inequalities and societal norms. For women, digital spaces can be both empowering and perilous. While access to information and platforms for expression can enhance their voices, they are also disproportionately targeted by cyber harassment and gender-based violence. Legal protections exist, but are often inadequately enforced. For instance, despite laws against online harassment in India and Bangladesh, many victims hesitate to report incidents due to fear of stigma or lack of faith in law enforcement. Youth also experience unique challenges in navigating digital rights. Many young people engage with technology as a primary means of communication and education; however, they are often subject to strict content regulations and surveillance measures that can stifle their creativity and freedom of expression. In Nepal, youth-led movements advocating for environmental issues have faced backlash under vague provisions of existing laws that restrict online speech. Ultimately, while legal frameworks aim to protect

marginalised groups, their actual impact is frequently diluted by societal attitudes and inadequate enforcement mechanisms.

Actual implementation data

Understanding the actual implementation data surrounding digital rights reveals a stark contrast between legislative intent and reality.

1. In India, despite the Supreme Court's recognition of internet access as a fundamental right, reports indicate that the country leads globally in internet shutdowns—over 100 documented instances in 2021 alone. These shutdowns often occur during protests or civil unrest, disproportionately affecting marginalised communities who rely on digital connectivity for information and advocacy.
2. In Bangladesh, implementation data from civil society organisations show that while internet penetration has increased significantly under the "Digital Bangladesh" initiative, corresponding rises in surveillance practices have led to increased self-censorship among users. The Digital Security Act has been invoked multiple times against journalists and activists; data reveals that a total of 1500 cases were filed under this law within its first three years of enactment. The Bangladesh police filed nearly 1300 cases under the previous law, the ICT.[23]
3. In Sri Lanka, following the introduction of the Online Safety Act, there has been a notable uptick in content moderation actions by social media platforms operating within the country. Reports suggest that many users are now more cautious about their online expressions due to fears of repercussions under this new legislation.[24] This data underscores a critical gap between policy aspirations and lived experiences—highlighting an urgent need for more robust monitoring mechanisms to ensure that digital rights are not merely theoretical but actively protected.
4. In Nepal, the implementation of digital rights has faced significant challenges, particularly in the wake of the proposed Information Technology Bill in 2020. This bill sought to impose strict regulations on social media usage and grant authorities extensive powers to block platforms without sufficient oversight. Civil society organisations and youth activists mobilised against these provisions, highlighting the potential infringement on freedom of expression

[23] https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951

[24] https://www.amnesty.org/en/latest/news/2024/01/sri-lanka-online-safety-act-major-blow-to-freedom-of-expression/

and the right to information. Their efforts included protests, public awareness campaigns, and advocacy initiatives that successfully raised national awareness about the risks associated with the bill.[25] Despite these challenges, Nepal has seen a growing movement advocating for digital rights, particularly among youth who are increasingly using social media to voice their concerns on various issues, including environmental protection and social justice.[26] However, the ongoing tension between government regulation and civil liberties remains a critical area for monitoring, as the balance between security and freedom continues to evolve in the digital landscape of Nepal. This dynamic illustrates how local activism can influence policy decisions and underscores the importance of vigilance in protecting digital rights amidst changing legal frameworks.

Civil Society Critiques

Civil society organisations and NGOs play a vital role in critiquing the implementation of digital rights across South Asia. Their insights often highlight significant gaps between legal frameworks and actual protections afforded to users. In India, groups like Article 19 advocate for freedom of expression by documenting instances where laws are misused to silence dissent. They argue that while laws like the Information Technology Act aim to protect users, they are frequently weaponised against activists and journalists under vague definitions of "hate speech" or "national security." In Bangladesh, organisations have raised alarms about the chilling effects of the Digital Security Act on free speech. They emphasise that many individuals refrain from expressing dissenting opinions due to fear of legal repercussions—a trend that undermines democratic engagement. These critiques underline a crucial point: civil society's role is not just to defend digital rights but also to hold governments accountable for their commitments to uphold these rights effectively. By amplifying marginalised voices and advocating for transparency in legal processes, civil society contributes significantly to fostering an environment where digital rights can flourish for all individuals.

25 https://www.b360nepal.com/detail/10395/in-nepal-new-laws-policies-and-mechanisms-relating-to-privacy-are-proposed-but-without-adequate-public-discourse

26 https://digitalrightsnepal.org/newsletter/digital-rights-weekly-year-3-issue-39/

What can citizens do?

Practical Protection Strategies

Protecting your digital rights starts with being proactive and informed. Keep detailed records of any concerning incidents or potential violations you encounter online. This documentation can be crucial if you ever need to report issues to authorities or seek legal help. Understanding how different platforms protect (or don't protect) your privacy is equally important. Take time to explore and adjust your privacy settings on social media and other digital services you use.

Building connections with digital rights organisations in your country can provide valuable support and resources when you need them. These organisations often offer guidance, legal assistance, and community support for those facing digital rights violations. They can help you understand your rights and the specific protections available in your country.

Encryption and privacy-enhancing tools are your digital armour – where legally permitted, use them to protect your communications and personal information. Regular security check-ups of your online accounts are like digital health examinations – they help prevent problems before they occur. This includes updating passwords, enabling two-factor authentication when available, and reviewing which apps and services have access to your information.

Remember, protecting your digital rights isn't just about individual actions – it's about being part of a larger community that values and defends these rights. By staying informed and taking these practical steps, you're not just protecting yourself in the present, you're also ensuring yourself against any new technologies that emerge in the near future. With the advancement of generative AI and other new technologies, it would be prudent to remember the lessons learned in this module. Module 3 will elaborate on the types of protection you can undertake to ensure digital security.

To summarise, it's important to:

1. Maintain detailed records of digital interactions and potential violations
2. Understand platform-specific privacy policies and terms of service
3. Build relationships with digital rights organisations and legal resources
4. Use encryption and privacy-enhancing tools where legally permitted
5. Monitor account security and privacy settings regularly

Engaging with Digital Rights

We will now consolidate our learning through **group discussions**, **analytical exercises**, and **action planning**. These activities are designed to reinforce the concepts covered in the previous chapters while providing practical, relatable examples that will help you remember and apply your knowledge of digital rights.

Group Discussions

- **Digital Rights in Your Context**: Discuss how digital rights manifest in your daily life. Share personal experiences or observations regarding internet access, freedom of expression, or privacy concerns. How do these rights affect women, youth, and marginalised groups in your community?
- **Impact of Legal Frameworks**: Reflect on the legal frameworks discussed in Chapter 3. How effective do you think these laws are in protecting digital rights? Are there any specific laws that you believe need reform? Why?
- **Case Studies Reflection**: Review one of the case studies from Chapter 2 (e.g., the movement against internet shutdowns in India). What lessons can be drawn from this case? How can similar strategies be applied to advocate for digital rights in your own context?

Analytical Exercises

Analytical exercises will help deepen your understanding of digital rights and their implications. Here are some exercises you can undertake individually or in small groups:

- **Critical Analysis of a Law**: Choose a specific digital law from any of the countries discussed (e.g., India's DPDP Act or Bangladesh's Cyber Security Act). Analyse its provisions by answering the following questions:
    - What are the intended protections offered by this law?
    - Who might be disadvantaged or left unprotected by its implementation?
    - Are there any potential loopholes that could be exploited?
- **Scenario Evaluation**: Think of recent news articles you might have read recently, related to digital rights violations (e.g., a woman facing online harassment or a youth being denied access to educational resources). Try to identify which rights are being violated and propose potential actions that could be taken to address these violations.
- **Mapping Rights Interconnections**: Create a visual map that connects different digital rights discussed in the module (e.g., how freedom of expression relates

to the right to information and privacy). This exercise will help you see the interrelated nature of these rights and understand their collective importance.

Action Planning

Action planning empowers you to take what you have learned and apply it in real-world contexts.

- **Identify Local Issues**: Identify specific digital rights issues within their communities. This could include access disparities, online harassment, or a lack of awareness about digital rights.
- **Set Goals**: Once issues are identified, set clear, actionable goals for addressing these issues. For example:
    - Raise awareness about online safety among local youth.
    - Advocate for better enforcement of privacy protections.
    - Organise workshops on digital literacy for women.
- **Develop Strategies**: Discuss potential strategies for achieving these goals. This could involve:
    - Collaborating with local NGOs or community groups.
    - Creating informative materials (e.g., pamphlets, social media campaigns).
    - Hosting community events or webinars focused on digital rights education.
- **Create an Accountability Plan**: Establish a timeline and identify who will take responsibility for each action item. This accountability will help ensure that plans are implemented effectively.

By engaging in group discussions, analytical exercises, and action planning, you will solidify your understanding of digital rights and empower yourselves to advocate for these rights in your communities. The knowledge gained throughout this module can serve as a catalyst for positive change, ensuring that everyone—especially women and youth—can navigate the digital world safely and equitably.

Emerging Technologies

Asheef Iqubbal
Senior Research Associate

Introduction

What really comes to mind when we talk about emerging technologies?

Emerging technologies are innovative tools in early development stages. Not yet widely available, they have the potential to transform industries, human activities, and create new markets. These technologies span fields like information technology, biotechnology, nanotechnology, materials science, and energy, and are often seen as disruptors to existing systems. They are fast-growing and impactful, and they bring uncertainty due to their newness. Examples include artificial intelligence, machine learning, blockchain, distributed ledger technology, the Internet of Things, virtual and augmented reality, and quantum computing.

Though still evolving, emerging technologies already influence various industries and are expected to shape the future. In banking, for instance, emerging technologies can improve customer experience, reduce costs, and boost efficiency. Customers now increasingly engage with banks through digital channels, generating not only traditional data like transaction records but also vast volumes of alternate data, including emails, text and voice messages, images, and videos from customer service interactions and social media. By using big data and AI, financial institutions are now delivering highly personalised services, such as tailored loan offerings.

Similarly, AI is transforming e-commerce, benefiting women and youth by making online shopping safer, smarter, and more accessible. Machine learning analysis consumer behaviour to offer personalised recommendations, helping shoppers find products suited to their needs. AI combats credit card fraud, ensures secure transactions, and detects fake reviews, empowering women entrepreneurs and small businesses. AI-powered chatbots enhance customer service with instant, tailored support, making online shopping more efficient and engaging.

However, they also introduce risks and vulnerabilities, such as privacy violations, cybersecurity threats, regulatory compliance challenges, potential misuse of sensitive information, and bias, which can disproportionately impact marginalised communities, including women and youth. Further, the rapid pace of these technologies can lead to skill gaps and require significant investments in training and infrastructure.

What exactly are we going to cover in this module?

In this module, we will explore the potential benefits and challenges of emerging technologies like AI, privacy-enhancing tools, gig work[27], and related regulations. We will examine how these technologies impact sectors and communities, particularly marginalised groups like women and youth. Using case studies and real-world examples, we will explore their societal impact. Next, we will discuss policy responses to protect rights, update legal frameworks, and the role of women and youth in shaping these regulations. By the end, we will understand the opportunities and risks of emerging technologies and the need for inclusive regulation.

Artificial Intelligence (AI)

AI has been a buzzword, hasn't it? Let's deconstruct it first.

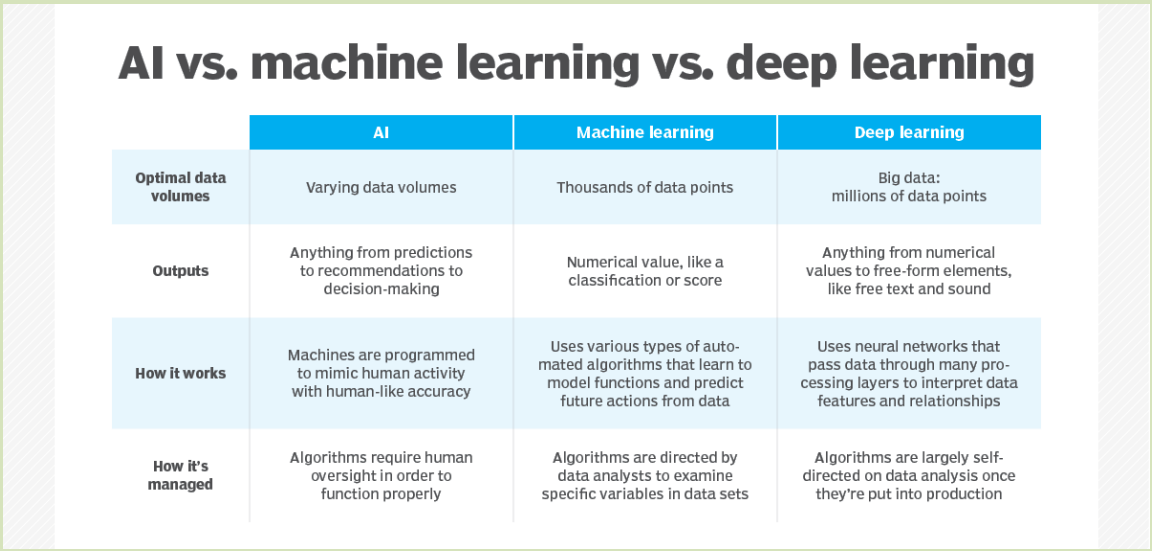
AI creates machines capable of reasoning, learning, and performing tasks requiring human intelligence or analysing large-scale data. AI is driven by machine learning (ML), deep learning, and natural language processing (NLP). Machine learning helps machines improve responses by analysing structured data and receiving feedback. Deep learning, an advanced form of ML, handles unstructured data like images or text through representation learning. NLP enables machines to interpret and respond to human language, bridging communication between humans and computers. AI's ability to learn and adapt makes it a transformative technology. By making devices smarter, AI reduces the need for direct programming. Even in its early stages, AI is transforming industries with applications like virtual assistants, analytics, and generative AI.

[27] While it may not fit directly into the emerging tech module, many young men and women are actively working in AI-driven environments, such as food delivery and cleaning services. Therefore, we are including it here with a focus specifically on how AI is used by these platforms for work management.

Understanding Different AI

Jeremy Howard, a data scientist, explains that AI constantly evolves and learns, like a child growing up at super speed. AI isn't magic—it's a tool that learns from us to improve our lives, one task at a time. Access the talk here: https://youtu.be/t4kyRyKyOpo?si=O9Q1V8ilu8QquaRh

AI, deep learning, and machine learning are often used interchangeably—learn the differences here: https://youtu.be/WP6z_X5d-Rw



AI vs. machine learning vs. deep learning

	AI	Machine learning	Deep learning
Optimal data volumes	Varying data volumes	Thousands of data points	Big data: millions of data points
Outputs	Anything from predictions to recommendations to decision-making	Numerical value, like a classification or score	Anything from numerical values to free-form elements, like free text and sound
How it works	Machines are programmed to mimic human activity with human-like accuracy	Uses various types of automated algorithms that learn to model functions and predict future actions from data	Uses neural networks that pass data through many processing layers to interpret data features and relationships
How it's managed	Algorithms require human oversight in order to function properly	Algorithms are directed by data analysts to examine specific variables in data sets	Algorithms are largely self-directed on data analysis once they're put into production

The next logical question is, "What can AI do?"

- ***Customer-facing AI use cases***

Deliver superior customer service: Conversational AI now enables real-time customer interactions. With text-to-speech and natural language processing (NLP), AI can respond instantly to text queries. Customers no longer have to wait for answers to FAQs or to complete purchases. Additionally, digital customer service agents can enhance satisfaction by providing advice and support to human agents.[28]

28 https://www.voicespin.com/blog/conversational-ai-for-customer-service/#:~:text=Conversational%20AI%20uses%20Natural%20Language,on%20the%20information%20retrieved%20from

Personalise customer experiences: AI effectively creates personalised experiences at scale through chatbots, digital assistants, and customer interfaces, delivering tailored experiences and targeted ads. For instance, Amazon reminds customers to reorder frequently purchased items and suggests related products.[29] McDonald's is leveraging AI and NLP to enhance its automated order-taking technology, enabling better integration of languages, dialects, and menu variations. Meanwhile, Spotify recommends new artists, and YouTube curates content based on user interests.

Smarten Up Smartphones: Facial recognition unlocks smartphones, while voice assistants like Siri, Alexa, Google Assistant, and Microsoft's Copilot use NLP to understand and respond to our commands. Companies also leverage machine learning in smartphone cameras to analyse and enhance photos, detect objects or faces, and use neural networks to predict and extend images beyond their borders.[30]

- ***Generative AI***

Arrival of generative AI, especially ChatGPT in 2022, catapulted it into the global spotlight, sparking an extraordinary wave of innovation and adoption. Generative AI creates new content, including text, images, videos, and music, by learning patterns from training data. By describing your needs in natural language, the model generates tailored outputs like text, images, or code. Generative AI is transforming industries with its versatility and potential. For example, Generative AI powers review highlights on e-commerce websites, making it easier for customers to understand what others are saying about a product. This feature summarises key product features and the most common customer sentiments into a short paragraph on the product detail page. It allows customers to quickly decide if a product meets their needs at a glance.[31]

Outputs from generative AI models can sometimes be indistinguishable from human-generated content, while at other times, they may appear slightly off. The quality of the model—such as ChatGPT, which outperforms earlier versions—and the relevance of the input play a significant role in determining the results. However, these outputs are not always accurate or suitable. For example, when a person asked DALL-E 2 to generate an image of a Thanksgiving dinner, it produced a scene where the turkey was garnished with limes and accompanied by what looked like guacamole. Similarly,

29 https://www.rejoiner.com/resources/amazon-recommendations-secret-selling-online

30 https://www.qualcomm.com/products/technology/artificial-intelligence/what-is-ai-faq/how-do-phones-use-ai#:~:text=Q%3A%20How%20do%20mobile%20phones,known%20as%20on%2Ddevice%20AI.

31 https://www.aboutamazon.com/news/innovation-at-amazon/how-amazon-uses-generative-ai

ChatGPT struggles with tasks like counting, solving basic algebra, and addressing the biases—sexist and racist—that are embedded in the internet and society.[32]

- ***Industry AI use cases***

Financial Services: India has nearly 190 million unbanked individuals excluded from mainstream financial services due to barriers like lack of credit history, education, language skills, and challenges in remote areas.[33] Credit scoring and loan eligibility assessment are critical for lenders but often rely on manual or rules-based processes driven by branch-level credit managers. AI can transform this by enabling alternate credit mechanisms that analyse hundreds of data points, such as customer behaviour, financial history, digital interactions, social media activity, and payment patterns, to produce comprehensive credit risk scores. This allows lenders to make more accurate decisions, minimise risks, and grow their portfolios. AI also enhances banking by using machine learning to detect suspicious transactions, applying predictive models for loan approvals, and leveraging ML in stock markets to forecast trends, suggest optimal trades, and execute algorithmic trading autonomously.[34]

Healthcare: The healthcare industry leverages intelligent automation and NLP for consistent data analysis, diagnosis, and treatment. Chatbots in remote healthcare appointments reduce the need for human intervention and speed up diagnosis. For example, in India, fewer than 20 percent of non-ICU hospital beds are closely monitored, as technology and continuous monitoring are typically limited to ICUs. Outside the ICU, vital sign monitoring is still largely manual, with nurses spending about 15 percent of their time collecting and documenting vitals. Studies indicate that up to 75 percent of hospital deaths occur in unmonitored areas outside the ICU. AI can automate vital sign collection and documentation, enhancing nurse productivity and allowing them to focus on critical patient care activities.[35]

It all seems like a dream, doesn't it? But lurking beneath the surface are serious risks that AI could amplify.

---

32 https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

33 https://www.outlookbusiness.com/opinions-and-blogs/why-access-to-credit-is-a-challenge-to-indias-financial-inclusion-7234

34 https://www.wipro.com/blogs/nikhil-goel/ai-in-digital-lending/#:~:text=AI%20can%20enable%20an%20ALTERNATE,in%20the%20past%20for%20credit

35 https://www.thenewsminute.com/atom/how-ai-based-remote-patient-monitoring-solution-changing-healthcare-india-91154

- ***Lack of Transparency***

The lack of transparency in AI systems, especially in complex deep learning models, poses a significant challenge. This opaqueness can obscure decision-making processes, leading to potential discrimination in critical sectors such as health, finance and employment. Transparency in AI deployment is crucial for building user trust. Users want to understand what decisions are being made with their data, how these decisions are reached, and why they are being made. They naturally distrust "black box" systems that do not provide clear explanations of their actions. For example, the algorithm, trained on a decade's worth of male-dominated resumes, favoured male candidates by downgrading applications containing the word "women's" and penalising graduates from women's colleges.[36] Without clear insights into how these systems operate, it becomes challenging to address and rectify these biases.

Actions

Demand Transparency Audits: Demand regular audits of AI systems to identify and address any obscurity in decision-making. Advocate for transparency in how data is used and ensure that diverse perspectives are considered in training data.

Raise Awareness: Educate others about the importance of transparency in AI, especially in sectors where decisions can have significant impacts on individuals' lives.

Push for Regulation: Support or engage in efforts to push for regulations that mandate transparency in AI systems, ensuring that users' rights and interests are protected against unintended harmful practices.

- **Bias and Discrimination**

AI systems can inadvertently perpetuate or amplify societal biases due to biased training data or flawed algorithmic design. For instance, in health insurance, an AI algorithm used to assess risk and determine premium rates might be trained on historical data that reflects disparities in healthcare access among different demographics. As a result, individuals from underrepresented groups may be unfairly labelled as higher risk, leading to higher premiums or denied coverage. AI bias in Southeast Asia has widespread consequences. On an individual level, biased AI systems

[36] https://www.ml.cmu.edu/news/news-archive/2016-2020/2018/october/amazon-scraps-secret-artificial-intelligence-recruiting-engine-that-showed-biases-against-women.html

can lead to unfair treatment, discrimination, and the denial of opportunities, particularly for marginalised communities. Societally, AI bias can deepen social divisions, erode trust in institutions, and hinder economic growth. In the context of election integrity, AI bias poses a serious risk to democracy. Generative AI models that rely on scraped data can unintentionally favour certain candidates or parties, undermining public confidence in the fairness of elections. For example, Google's Gemini AI faced backlash for being labelled a "woke AI" due to its tendency to present data with a perceived liberal bias, raising concerns about AI's neutrality in political matters.[37]

Systematic Exclusion
Algorithms are computational representations of social realities. Their assumptions and parameters reflect the knowledge and values of their designers, often excluding alternative perspectives. UNESCO's 2019 report "I'd Blush if I Could" highlighted gender disparities in AI: only 12 percent of AI researchers and 6 percent of software developers are women. Women hold 21 percent of technology roles at Google, with just 10 percent in machine learning. This underrepresentation risks creating technologies that neglect the needs of half the population. The dominance of men in AI design could undermine progress in gender equality, leading to systems that disadvantage women and gender minorities. Research reveals significant biases in AI, particularly in facial recognition and natural language processing. Studies show commercial facial recognition systems often misgender and misidentify female faces, with error rates as high as 34.7 percent for darker-skinned women compared to 0.8 percent for lighter-skinned men. In natural language processing, training data biases reinforce stereotypes, associating "doctor" with men and "nurse" or "receptionist" with women. Even when datasets capture a single identity attribute, accuracy declines at the intersection of multiple attributes. Research on intersectional biases highlights how these systems often fail to represent and serve marginalised identities.[38]

[37] https://www.businessinsider.com/google-gemini-woke-images-ai-chatbot-criticism-controversy-2024-2

[38] https://www.orfonline.org/expert-speak/from-data-to-deployment-gender-bias-in-the-ai-development-lifecycle

Actions

Monitor for Discrimination: Be vigilant about how AI systems are applied, particularly in sensitive areas like healthcare, employment, and finance. Users should report instances of unfair treatment or discrimination caused by biased AI systems.

Support Fair and Inclusive Policies: Engage in discussions and initiatives that advocate for fair and inclusive AI governance. Support policies that regulate AI deployment to ensure it does not disproportionately impact marginalised communities.

Stay Informed: Keep up-to-date with the latest developments in AI and its potential for bias. Users should educate themselves about the risks of AI and take proactive steps to mitigate its impact, such as using AI tools that prioritise fairness and diversity.

- ***Security and Privacy Concerns***

AI systems often rely on extensive datasets to train algorithms and enhance performance. This data often includes personal details, such as names, addresses, financial records, and even sensitive information like medical histories and Aadhaar, a digital identity card in India. The collection and processing of such information raises significant privacy concerns, especially regarding data security and unauthorised access. A major risk associated with AI-driven data collection is the potential for data breaches. With vast amounts of data stored and processed, there is an increased chance that it could be accessed or misused. Malicious actors are using AI tools to execute sophisticated attacks. For instance, a data breach recently occurred with Star Health, which exposed the health records of millions of users. AI's use in surveillance also raises privacy concerns. Facial recognition technology, for example, has been deployed by law enforcement agencies to identify and track individuals in public spaces. While this can aid in crime prevention, it also risks infringing on personal privacy, enabling authorities to monitor people's movements, social media interactions, and even biometric data like facial expressions—often without their consent. Such surveillance capabilities, if unchecked, could lead to privacy infringements, eroding public trust.

Actions

Review privacy policies: Always review the privacy policies of services or platforms using AI, especially those requesting sensitive information like medical histories or

digital identity data (e.g., Aadhaar in India). Ensure that clear, concise, and transparent consent is only being obtained.

Limit data sharing: Avoid sharing unnecessary personal information with AI platforms. Ensure that the data shared is relevant to the service being provided and is limited to what is necessary to fulfil the specific purpose.

Report suspicious activities: If you notice any suspicious or unauthorised use of personal data, report it to the relevant authorities or organisations.

Demand Privacy by Default: Demand that privacy settings be set to the highest level of protection automatically. This ensures that your data is always protected, with any additional privacy controls or permissions only activated when you explicitly choose to do so.

- ***Concentration of Power***

The concentration of AI development in the hands of a few large corporations and governments, due to their enormous resources, presents significant risks to equality and diversity in space. The current AI boom relies on two key factors: vast amounts of data and the computing power needed to process it. Unfortunately, both of these resources are primarily accessible to large companies.[39] When only a small number of powerful players dominate the development of AI technologies, their perspectives, priorities, and interests often shape the direction of innovation. This concentration of power can result in AI applications that cater mainly to the needs and values of these entities, potentially overlooking the diverse requirements of smaller businesses, underrepresented communities, or different cultural contexts. As a result, this could reinforce existing inequalities and limit the scope of AI's potential to benefit all of society.

For example, if only a few tech giants control the development and deployment of AI systems, they may prioritise solutions that align with their business models or market demands, which may not be relevant to other marginalised groups. This could lead to a lack of diverse voices and inputs in the development of AI, reducing innovation and creating solutions that are biased, narrow, or inaccessible to many people. A key debate surrounding AI is whether to support closed or open-source AI. Advocates of

[39] https://www.cnbc.com/2023/11/22/ai-is-giving-big-tech-inordinate-power-tech-execs-say.html

open-source AI – systems with publicly accessible components for study, use, modification, and sharing – argue that it fosters innovation, enhances transparency, and reduces market concentration. However, critics warn that open-source AI could pose safety risks and disadvantage certain AI companies in the competitive landscape.

Actions

Demand the promotion of decentralised, open, and collaborative approaches to AI development. Encourage the active participation of smaller companies, independent developers, researchers, and diverse stakeholders in the AI innovation process. Support open-source projects, public-private partnerships, and international collaborations to ensure that AI evolves in a way that serves a wider range of people and addresses various needs. Decentralised AI development will reduce the dominance of a few entities, create more opportunities for innovation, and ensure AI technologies reflect diverse values and priorities. This inclusive approach will foster the creation of ethical, equitable, and transparent AI solutions, benefiting society as a whole.

- ***Misinformation and Manipulation***

AI-generated content, such as deepfakes, plays a significant role in spreading false information and manipulating public opinion. For instance, during the 2020 U.S. presidential election, deepfake videos circulated on social media, misrepresenting candidates' statements and actions, thereby influencing voter perceptions. Efforts to detect and combat AI-generated misinformation are crucial for preserving the integrity of information in the digital age. In a Stanford University study on the dangers of AI, researchers stated: "AI systems are being used in the service of disinformation on the internet, giving them the potential to become a threat to democracy and a tool for fascism. From deepfake videos to online bots manipulating public discourse by feigning consensus and spreading fake news, there is a danger of AI systems undermining social trust. The technology can be co-opted by criminals, rogue states, ideological extremists, or simply special interest groups to manipulate people for economic gain or political advantage."

Further, the modern information landscape presents new challenges. With technological and social advancements, the ease and scale of information distribution have led to issues of overload and manipulation. Generative AI now amplifies this, creating synthetic content at an unprecedented rate and, through social media, spreading it rapidly. This content influx not only risks cognitive overload but also biases users toward information that aligns with their existing beliefs. Consequently, the ideal

of "access to information" now requires careful balancing to prevent selective engagement and the spread of harmful biases.[40] Generative AI has been known to produce hallucinations, which are incorrect or misleading results generated by AI models. These errors can occur for various reasons, including insufficient training data, incorrect assumptions made by the model, or biases in the data used to train the AI. Such hallucinations can be particularly problematic in AI systems used for critical decision-making, such as medical diagnoses or financial trading, as they may lead to harmful or costly consequences. [41]

Actions

Verify Content Sources: Always check the credibility of the content you encounter, especially videos or images that seem too dramatic or sensational. Use trusted sources to verify facts before sharing or forming opinions.

Educate on AI Manipulation: Stay informed about AI-generated content, particularly deepfakes. Understand the potential risks and how to recognise manipulated media to avoid being misled or spreading false information.

Promote Digital Literacy: Encourage digital literacy, both for yourself and others. This includes understanding how AI can be used to manipulate content and how to critically assess the information you encounter online.

Report Misinformation: If you come across deepfakes or other AI-generated misinformation, report it to the platform administrators. Many social media platforms are enhancing their tools to detect and remove harmful content.

Support AI Regulation: Advocate for stronger regulations to prevent the misuse of AI in spreading disinformation. Push for policies that require transparency in AI-generated content and hold relevant parties accountable for its impact on public opinion.

[40] https://www.americanactionforum.org/insight/open-source-ai-the-debate-that-could-redefine-ai-innovation/

[41] Investigative reporter Ariel Bogle discusses the risks posed by deepfakes with Nour Haydar: https://www.theguardian.com/australia-news/audio/2024/jun/18/the-deeply-troubling-world-of-deepfakes-full-story-podcast

AI Regulations

For much of the past decade, public concerns around digital tech have centred on personal data privacy. People grew uneasy with how companies tracked them online, gathering sensitive information like credit card details and addresses. Ads that followed users across the web after casual searches only heightened this discomfort, along with rising worries about identity theft and fraud. In response, regulations like India's Digital Personal Data Protection Act emerged to give users more control over their data. These measures have sparked intense debate. Some argue that strict data controls stifle economic growth and disadvantage smaller companies, making it harder for them to compete with global giants. Others contend that limited regulatory oversight risks violating fundamental rights, such as privacy and free expression. Despite these contestations, global policymakers seem to agree on one thing—we must leverage the power of emerging technologies while mitigating their risks.

Now, the conversation is shifting toward how data is used in AI-driven systems, from diagnosing diseases to approving loans. With AI embedded in products, services, and decisions, regulators are focusing on ensuring these systems are fair and trustworthy. In 2022, more than 30 AI-related laws were enacted across over 100 countries. The launch of ChatGPT later that year marked a turning point, pushing generative AI into the spotlight. Alongside its rapid rise, concerns emerged about bias, misinformation, copyright infringement, and its potential effects on labour markets. This moment also reflected a convergence of key developments: significant advances in machine learning, the powerful capabilities of large language models, and the pervasive influence of social media. These factors heightened fears among policymakers, prompting some nations to introduce new regulations.

The EU, once again leading on policy, has proposed an AI regulatory framework to promote transparency and protect consumers in this rapidly evolving space. As reliance on AI—particularly machine learning—grows, so do the risks. Companies need to shape guidelines for algorithms, as analytics increasingly influence critical decisions like loan approvals and assessments of criminal recidivism. Concerns about hidden biases in these systems continue to rise, along with worries about the inherent opacity of machine learning models. There is also mounting concern over whether AI tools developed for one group of people can accurately and safely make decisions for other populations.

When advocating for policymaking, we might consider focusing on five categories of risks that are particularly pertinent from a regulatory perspective[42]

Malicious Uses	The creation and distribution of harmful AI-generated content that could violate legal rights or threaten public order and safety.
Algorithmic Discrimination	Risks arising from unreliable or unrepresentative datasets in AI systems, leading to financial losses, loss of opportunity, and threats to fundamental rights.
Transparency Failures	Lack of adequate disclosures on AI decision-making, training data, and information asymmetry, potentially threatening privacy and other rights.
Systemic Risks	Dependence on a few AI systems in critical sectors (e.g., finance, healthcare, national security) could lead to widespread disruptions with catastrophic effects.
Loss of Control	Absence of human oversight in autonomous AI systems could lead to unintended consequences and pose threats to national security and public safety.

Actions

A balanced approach is needed to mitigate risks without stifling innovation. Flexible frameworks that adapt to emerging technologies can achieve this while protecting rights and safety. Collaboration among regulators, industry, and researchers is crucial to develop solutions that support innovation, competitiveness, and responsible AI. Thus, we should demand that AI systems posing unacceptable risks—such as enabling mass surveillance or systematic social behaviour evaluation—be categorically banned. High-risk AI systems, including those used in critical sectors such as finance, food and health, must adhere to strict transparency and monitoring requirements. These systems should undergo rigorous risk assessments and demonstrate compliance with robust security and data protection standards. For AI systems with limited or minimal risk, lighter requirements should apply, but transparency and clear information-sharing are essential to build public trust in these technologies.

[42] https://carnegieindia.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india
Also listen to this policy podcast on the AI Act: https://www.youtube.com/watch?v=pYJqit9MhgY&t=4s

Privacy Enhancing Technologies

Laws such as the Digital Personal Data Protection Act and the General Data Protection Regulation aim to protect user privacy through principles like consent, purpose limitation, and data minimisation. These regulations emphasise that consent must be free, fair, unequivocal, voluntary, and given without any form of coercion or undue influence. Consent should also be informed, meaning individuals must understand the nature and consequences of what they are agreeing to. However, in South Asia, particularly among women, limited digital literacy has hindered the effectiveness of these laws, despite their good intentions. Additionally, a lack of awareness regarding data collection, processing, and sharing further complicates matters. Users may not realise that their data is being used for profiling, which can disproportionately affect marginalised social groups. Further, data breaches are frequently in the news, exposing sensitive information such as credit card details and personal records.

Thus, it is crucial to advocate for regulators to enforce the use of privacy-enhancing technologies (PETs), particularly in high-risk sectors such as food, health, and banking, where personal and sensitive data are frequently collected and processed. PETs are a set of tools and methodologies designed to protect sensitive data while ensuring that the confidentiality and integrity of the information are maintained. These technologies are especially important as they maintain analytical values of the datasets, without exposing or compromising individuals' private information. PETs work by implementing various techniques such as encryption, which ensures that data is unreadable without the proper decryption key; anonymisation, which removes identifying details from datasets to protect individual identities; and access controls, which restrict data access only to authorised users. Similarly, solutions like differential privacy allow for the sharing of aggregated data without revealing details about specific individuals, while synthetic data generation creates artificial datasets that mirror real data but do not contain actual personal information.

Women and youth should demand privacy-enhancing technologies for key reasons. They are vulnerable to online harassment and gender-based violence, with women often facing abuse, stalking, and exploitation on digital platforms. Privacy technologies like end-to-end encryption and data anonymisation protect personal information and communications. As digital engagement increases, the risk of data breaches, identity theft, and cyber exploitation rises, especially for young people navigating online spaces. Privacy technologies safeguard sensitive data such as financial details and location tracking. Moreover, women and youth are often targeted by biased AI systems that perpetuate gender and age discrimination in areas like job recruitment,

healthcare, and finance. By demanding privacy-enhancing technologies, individuals can better protect their data and avoid being subjected to discriminatory algorithms. These technologies also give individuals control over their data, enabling explicit consent for its use, preventing exposure to surveillance or data exploitation. This is especially important for women and youth, who may have limited awareness of the full extent of data collection.

Actions

Demand the Use of PETs: Demand policymakers to introduce regulations that require the adoption of PETs in high-risk sectors, particularly in services handling sensitive personal data. This should include encryption, anonymisation, and differential privacy to protect individuals' personal information while maintaining the integrity and usefulness of datasets.

Demand Platform Accountability: Strengthen regulations around data security practices, holding platforms accountable for breaches and mandating transparent reporting of incidents. Platforms should be required to implement rigorous data protection measures and penalise those that fail to adequately protect user information.

Gig Workers

What is gig work?

Some work arrangements are defined by the relationship between workers and the entity that pays them. Standard employment involves a long-term employer-employee relationship, where workers receive hourly, monthly wages or a yearly salary. Beyond this, many work arrangements are temporary or project-based, with workers hired for specific tasks or set time frames. In some cases, workers may have an employer, but the company issuing their payment is separate from the company where they perform their work. These types of arrangements, often called alternative or non-standard work arrangements, include freelancing, gig work, self-employment, and subcontracting. Gig and platform work has become a significant source of employment both globally and in India. According to NITI Aayog, the sector employed 7.7 million workers in 2020, a figure projected to triple to 23.5 million by 2029–30.[43] This growth has brought about a dramatic transformation in work arrangements, introducing new challenges related to the use of big data in employment.

[43] https://www.ilo.org/publications/expansion-gig-and-platform-economy-india-opportunities-employer-and

The technological framework and socio-economic conditions inherent in the gig economy create significant power imbalances between workers and platforms or users. As a result, gig workers are often compelled to trade their privacy for opportunities, from the moment they are hired to their everyday experiences on the job.[44]

These work arrangements exist across various sectors, including food service, delivery roles in e-commerce, and cleaning services. For example, food delivery services have become major employers in urban and peri-urban areas, facilitating restaurant-to-customer food deliveries through a network of delivery workers. The job primarily requires a motorbike or bicycle and a smartphone with internet access. While this arrangement may appear straightforward, it poses significant challenges for delivery workers, or "riders," who are typically paid per delivery. These platforms classify them as "independent contractors" or "delivery partners," not traditional employees. As a result, they lack access to standard labour rights related to pay, working hours, conditions, and collective bargaining.[45]

Challenges in the Gig Economy

Women's participation in the gig and platform economy is increasing, especially in roles not tied to a specific location. However, many platforms, such as ride-hailing and delivery apps, remain male-dominated. Although women are joining the gig economy, they often perform similar roles to those in the traditional workforce, with minimal shifts in job types. For example, women predominantly fill roles as beauticians on gig platforms, echoing gender norms from traditional employment structures. Both male and female gig workers face common challenges, particularly around the terms and conditions imposed by platforms. Further, many workers are unaware of the extent of data being collected, such as real-time tracking. As one expert noted, "many gig workers are confused about how data sharing and algorithms operate, leaving them unclear on issues of consent and data use".

Concerns about the opacity in platform work are growing as AI plays an increasingly dominant role in gig economy platforms. These platforms rely heavily on machine learning models—often described as "black boxes" due to their opaque decision-making processes—to manage tasks, assign jobs, and evaluate worker performance. As a result, it leaves workers without explanations for rejected work, poor ratings, or terminations. The problem is further exacerbated by the lack of effective grievance or

[44] The Hidden Cost of Gig Work: Unpaid Labour and Its Impact on Platform Workers: https://www.youtube.com/watch?v=fdJFfhkejAU&t=12s

[45] To learn more specifically about the status of food industry workers, listen to this AI-generated podcast: https://drive.google.com/drive/folders/103Qhv_gHqIzxd9wyUVM3zmo4zrRUzdt5

dispute redressal mechanisms.[46] This lack of meaningful human interaction can have psychosocial impacts on workers. Human-to-human engagement in the workplace creates connection, empathy, and a sense of belonging—factors that contribute to fulfilment. When these interactions are replaced by faceless algorithms, workers may feel reduced to mere data points, eroding their sense of individuality and worth within the system. For example, Zomato riders have reported receiving calls warning them to log back into the app or risk losing incentives. This surveillance not only serves commercial objectives but also shapes behavioural traits.

Equal Stakeholder?
Workers generate a constant stream of monetisable data for platforms without receiving proportionate compensation. For example, Uber drivers create valuable data points for the central platform, enabling insights into braking frequency, acceleration speed, traffic patterns, and user demand. This data drives algorithm-based price determination and is critical for business planning, optimising operations, accelerating decision-making, maximising profits, and adapting to dynamic conditions. Further, platforms can sell these insights to other companies for advertising or commercial purposes, generating further revenue.[47]

Algorithms are often designed to prioritise efficiency and profit over the well-being of workers, creating a work environment characterised by unpredictability and stress.[48] This constant state of flux generates feelings of insecurity, as workers grapple with diminished autonomy and potential invasions of privacy caused by excessive data monitoring. Gig workers are continuously monitored through the app, which provides detailed, real-time data on their location, time spent on tasks, and breaks taken. For example, Dunzo's delivery partner agreement states that, in addition to tracking workers' geo-location data while services are being provided, the company may also use this information for purposes such as "safety, security, technical, marketing, and commercial activities."[49] The lack of transparency in algorithmic decision-making compounds these challenges. Workers are often left in the dark about why certain jobs are assigned to them or why their performance is rated a certain way, making it difficult to appeal or correct perceived injustices.

46 https://purl.stanford.edu/fc567cc8525
47 https://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation
48 https://giswatch.org/node/6202
49 https://www.dunzo.com/terms#partner_terms'

For instance, some female gig workers believe that certain areas are geofenced for their safety, preventing them from receiving ride or delivery requests in those locations. This raises important questions about which areas are restricted, who determines these designations, and whether such measures are truly effective in enhancing worker safety. The cumulative effect of these factors is a workforce at risk of withdrawal and burnout. The inability to engage in fulfilling activities, coupled with a sense of being undervalued and over-monitored, can significantly impact the mental health and well-being of platform workers. Lack of transparency in the platform's design causes workers to question decisions around ride allocation, penalties, and other rules. While technology can enhance efficiency, it must not come at the cost of worker dignity and mental health. A balanced approach that integrates the benefits of automation with the irreplaceable value of human connection is critical for ensuring that platform work remains equitable and empowering.[50]

I have heard some debates about gig workers and welfare—would it be helpful for them?

The gig economy promotes the idea of equal stakeholders: tech companies, service providers, and consumers. However, gig platforms often operate more like employers, controlling work conditions rather than merely connecting service providers to consumers. India's gig platforms enforce similar practices, requiring workers to wear branded uniforms or use specific delivery bags, with financial penalties for non-compliance. More significantly, workers must follow income and incentive structures set by the platform, which often necessitates working over 8 hours a day, including weekends, to earn a sustainable wage. Gig companies avoid identifying as employers to minimise expenses they would otherwise bear for worker protection and risk mitigation. This issue has fueled global legal debates on whether gig platforms should be classified as employers, with gig workers as employees.

In the United States, California has passed Assembly Bill 5, mandating that drivers and delivery partners be classified as employees. The law applies a test to determine if gig workers operate under the "control and direction" of the platform, a criterion previously upheld by the California Supreme Court. Many Indian states, including Rajasthan and Karnataka, are extending certain welfare entitlements to platform-based gig workers. Claimed as the first of its kind in India, the legislation holds platforms accountable for contributing to this goal. For example, the Rajasthan Platform-Based Gig Workers (Registration and Welfare) Act, 2023, takes its cue from the Code on Social

[50] Watch this video to learn more: https://www.youtube.com/watch?v=naOKu92aiig

Security, 2020, which proposed a similar approach. The union labour ministry and other states are considering similar measures in India. These laws provide minimal safeguards for worker welfare but fail to address unfair practices such as the lack of transparency in platform design, inadequate data security measures, and violations of privacy.

Actions

Demand Legal Protections for Gig Workers: A robust legal framework is essential to safeguard gig workers' rights. This framework should include the right to privacy, protections against algorithmic bias, and access to human-mediated decision-making processes. Labour and privacy laws must work together to uphold shared values, ensuring the dignity and empowerment of gig workers. Platforms must be mandated to:

- Ensure transparency in algorithmic decision-making.
- Incorporate mechanisms for human oversight.
- Create opportunities for meaningful human interaction within platform work.

Support Gig Workers in Collective Bargaining: Gig workers must have the right to collectivise and manage their data, enabling them to negotiate its use and share in its benefits. Strengthening unions like the All-India Gig Economy Workers Union is essential to amplify workers' voices and enhance their bargaining power. Expanding and publicising such initiatives will play a key role in improving worker welfare and ensuring fair treatment within the gig economy.

Cybersecurity and Digital Safety

Krishaank Jugiani, *Senior Research Associate*
Deepmala Ghosh, *Research Associate*
Sobhan Guha, Programme Associate

This module is designed to equip women and youth in South Asia with foundational knowledge and practical skills in cybersecurity, enabling them to secure their digital environments, recognise risks, and advocate for inclusive digital rights and policies.

Module Objectives:

1. **Awareness:** Understand the importance of cybersecurity and its impact on personal and professional digital spaces.
2. **Risk Mitigation:** Learn to identify common cybersecurity risks, including data breaches, and develop strategies to mitigate them.
3. **Safe Navigation:** Acquire hands-on experience in safe online practices and secure digital navigation.
4. **Digital Rights:** Explore the intersection between cybersecurity and digital rights, with an emphasis on the importance of advocacy and inclusive policies.
5. **Collaboration:** Build networks for collaborative efforts toward safer digital environments.

Introduction to Cybersecurity

- What is Cybersecurity?

Cybersecurity is all about keeping our digital world safe. It means:

- **Protecting systems and data**: Ensuring your digital devices and information are protected from unauthorised access
- **Preventing cyberattacks**: Stopping attempts to damage or steal data.
- **Keeping things private and working properly**: Making sure that you have access to your data in a confidential, correct, and available setting.

The main goal is to ensure that all technology we are using for our daily activities remains reliable, safe and functional.

Cybersecurity measures involve various techniques, tools, and practices designed to prevent, detect, and respond to threats. With the rapid increase in digital connectivity, cybersecurity has become essential to protect personal and sensitive data across both individual and organisational levels.

- Key Cybersecurity and Digital Safety Threats

1. **Malware**: Malware is malicious software designed to infiltrate or damage devices, networks, or systems. It includes viruses, worms, Trojans, ransomware, and spyware. Once installed, malware can disrupt services, steal information, or take control of the targeted system, often leading to significant losses.
2. **Phishing**: Phishing is a deceptive practice where attackers use fake emails, messages, or websites to trick users into revealing personal information, such as passwords, credit card numbers, or social security numbers. Often, phishing attacks impersonate trusted institutions to gain the target's trust.
3. **Identity Theft**: This is the unauthorised use of someone's personal information, typically to commit fraud or theft. Cybercriminals may use stolen information to impersonate the victim, make purchases, or even commit crimes, which can result in significant personal and financial harm to the individual affected.
4. **Social Engineering**: Social engineering involves manipulating people into giving away confidential information or taking unsafe actions. Rather than exploiting technical vulnerabilities, social engineers target human psychology, exploiting trust or fear to gain access to sensitive information or systems.
5. **Hateful speeches** or content directed at an individual or group of individuals based on their religion, caste, race, ethnicity, gender, socioeconomic background, etc. These speeches or content are created with the intention of causing emotional or psychological harm.
6. **Trolling:** Making uninvited comments on social media or other online platforms is known as trolling. It could entail making sexually offensive remarks, lying, and providing inaccurate information. Additionally, trolling can be carried out through the creation of phoney photos or memes.
7. **Cyberbullying** is the deliberate and repeated use of digital platforms to harass, threaten, or humiliate someone, often causing emotional distress and harm.

8. **Doxxing** is the act of intentionally revealing another person's personal information on the internet with malicious intent. This could encompass confidential information like their residential address, financial account details, contact number, ID card particulars, or details regarding their relatives.
9. Abusers could also employ **deepfakes**, which are synthetically created images or videos, to control the victim's identity. They might generate deceptive content by overlaying the victim's face onto someone else's body or producing sexually explicit material.

These threats can appear both ways, either in isolation or together, increasing the possibility of damage. For example, a phishing attack might deliver malware, which can then facilitate identity theft for further social engineering attacks.

Cybersecurity Incidents in South Asia: Gendered Implications
In South Asia, the digital divide and gender inequalities create distinct cybersecurity challenges, particularly affecting women and marginalised communities. Cybersecurity incidents such as online harassment, doxxing (publishing private information without consent), and identity theft have disproportionately impacted women, creating barriers to their digital participation and personal safety. Moreover, many women in the region face cyber threats like revenge porn, blackmail, and stalking. These threats can lead to social and psychological impacts, sometimes causing victims to withdraw from online spaces altogether. Recognising these gendered implications is crucial for developing inclusive cybersecurity strategies that provide safer online environments for all users, particularly those vulnerable to gender-based cyber incidents.

Data Breaches and Mitigation Strategies

A **data breach** occurs when sensitive, confidential, or protected data is accessed or disclosed without authorisation. This can involve personal data, financial records, healthcare information, and other valuable information, often resulting in financial loss, identity theft, and privacy invasion. Data breaches typically happen due to weak security practices, unpatched software vulnerabilities, social engineering attacks, or insider threats. Hackers exploit these weaknesses to gain unauthorised access to data for malicious purposes or financial gain.

- Best Practices for Securing Personal Devices: Password Management, Software Updates, Multifactor Authentication.

1. **Password Management**: Creating and using strong, unique passwords for different accounts is essential. A password manager can help generate and store complex passwords, reducing the risk of password reuse and brute-force attacks.
2. **Software Updates**: Keeping software and operating systems up to date is critical, as updates often include patches for security vulnerabilities that attackers might exploit. Automatic updates or regularly checking for new updates ensures that security loopholes are promptly fixed.
3. **Multifactor Authentication (MFA)**: MFA adds an extra layer of security by requiring additional verification steps, such as a text message code or biometrics, beyond just the password. This reduces the risk of unauthorised access even if passwords are compromised.
4. **Biometric Authentication:** Fingerprint scanning, facial recognition, and even voice recognition are gaining more widespread. Many smartphones today use these methods to access a user. Those biometric systems are available to be highly secure because they are based on a unique physical trait of the user.
5. **One-time passwords (OTPs):** These methods replace traditional passwords and send a one-time code to the user via email (or through SMS). These credentials are only valid for one use, which increases security by eliminating vulnerabilities stemming from password reuse.
6. **Device-based Authentication:** It enables users to verify using secure elements in devices (smartphones or security keys like YubiKey), without involving passwords. These methods are dependent on the hardware and protect against common attacks really well.

As representatives of the community and rights group, CSOs can

- *Advocate for Stronger Cybersecurity Laws and Regulations:* advocate for laws that mandate stronger protective measures, particularly around public networks and data security. For example, this includes calling for regulations that mandate robust privacy protection standards and legal consequences for those who exploit vulnerabilities.
- *Promote Digital Literacy and Awareness Programmes:* CSOs can advocate and also organise educational programmes that focus on digital literacy and safe internet practices. This could include teaching individuals how to recognise cyber threats, use VPNs, and protect their data when using public networks.
- *Advocate for Better Accountability for Tech Companies:* advocate for transparency and accountability from tech companies to ensure they implement

clear and transparent policies and use safeguards like enhanced spam filters, stronger identity verification processes.

- *Demand Greater Consumer Protection:* advocate for laws that better protect consumers from cyber threats and other forms of fraud. This can include requiring financial institutions to provide greater support for users who fall victim to cyber threats, mandating stronger safeguards for sensitive personal data, and developing easier methods for users to report cyber threat attempts.

Legal Frameworks, Recourse and Advocacy in Combating Cyberthreats

Each South Asian country has implemented or is developing laws to address cyber threats and regulate digital spaces:

- **India**: The **Information Technology (IT) Act, 2000** governs data protection, cybersecurity, and online content regulation.
- **Sri Lanka**: The **Computer Crimes Act** is a foundational law for prosecuting cyber crimes
- **Bangladesh**: The **Digital Security Act** addresses cybercrime
- **Nepal**: The **Electronic Transactions Act** provides a framework for digital governance

National-Level Recourse

1. *Online Reporting Mechanisms:* Many countries, such as India, with its **National Cyber Crime Reporting Portal**, offer platforms for victims to report cybercrimes.
2. *Civil and Criminal Remedies:* Victims can seek compensation through civil suits or pursue criminal cases under laws addressing cybercrime.

International Protections

1. **Human Rights Frameworks**: Instruments like the **Universal Declaration of Human Rights (UDHR)** and the **International Covenant on Civil and Political Rights (ICCPR)** safeguard the right to privacy and freedom of expression. Many countries are signatories to these frameworks. These can be leveraged to hold states accountable for cyber-related violations.
2. **Global Advocacy Platforms**: Forums such as the **Internet Governance Forum (IGF)** provide avenues to raise awareness and seek international support for digital rights issues.

Cybersecurity and Digital Rights

Digital rights are the entitlements that individuals have to safely and fairly access, utilise, generate, and distribute digital materials. These rights are fundamental in democratic societies, covering privacy, security, and freedom of information.

Cybersecurity plays a critical role in upholding digital rights, as it ensures the protection of personal data, online identities, and digital infrastructures from malicious threats. A secure digital environment is essential for preserving privacy and safeguarding individuals' ability to freely access and share information without fear of surveillance or exploitation.

In the context of digital rights, cybersecurity measures must be designed to respect human rights, ensuring that they do not disproportionately infringe upon freedoms while addressing security risks.

Key Digital Rights and Their Relation to Cybersecurity

- *Right to Privacy:* Cybersecurity ensures the confidentiality of personal data by protecting it from breaches and unauthorised access. Strong encryption, secure communication channels, and data protection measures are critical to maintaining privacy.
- *Right to Security:* Individuals have the right to a secure digital environment free from cyber threats like hacking, phishing, and malware. Cybersecurity practices like two-factor authentication and firewalls help safeguard this right.
- *Freedom of Information:* Secure and fair platforms prevent the manipulation of information and ensure that users can access reliable and unaltered content.
- *Freedom of Expression:* Secure digital spaces protect users from harassment and cyberbullying, enabling them to express themselves without fear. Cybersecurity tools like privacy by design play a vital role here.
- *Right to Non-Discrimination:* Inclusive cybersecurity frameworks help create safe digital spaces for marginalised communities, ensuring they are not disproportionately affected by cyber threats or surveillance.
- *Right to Digital Literacy:* Cybersecurity education empowers individuals to navigate the digital world safely, equipping them with skills to protect their rights and identities online.

Data breaches pose significant threats to digital rights, often exposing personal information to malicious actors and compromising individuals' privacy and security.

Balancing Security and Rights: The Role of Civil Society Organisations

Civil Society Organisations play a critical role in advocating for a balanced approach to cybersecurity that ensures robust security measures while upholding fundamental digital rights. This includes:

- *Advocacy for Rights-Based Cybersecurity Policies:* CSOs lobby governments and industries to develop cybersecurity frameworks that respect privacy, freedom of expression, and access to information.
- *Awareness and Capacity Building*: They organise workshops and training sessions to educate individuals, including marginalised groups, about cybersecurity best practices and their rights in the digital space.
- *Policy Research and Recommendations*: CSOs also produce evidence-based research to highlight the impact of cybersecurity measures on human digital rights and propose policy solutions that balance security and convenience.
- *Digital Inclusion Initiatives:* They work with other NGOs undertaking initiatives that aim to address accessibility, affordability, and digital literacy of individuals and communities, including marginalised groups.
- *Monitoring and Accountability:* They act as watchdogs, holding governments and corporations accountable for cybersecurity practices that may infringe on individual rights.

Role of Youth and Women-Led Organisations

Youth and women-led organisations are also pivotal in shaping inclusive cybersecurity practices and ensuring equitable digital rights. They can

- advocate for cybersecurity policies that promote innovation and creativity without excessive restrictions
- mobilise women and youth to demand secure and open digital spaces through campaigns and grassroots movements
- equip women and youth with digital literacy and cybersecurity skills to navigate and safeguard online environments.
- advocate for addressing gendered threats like online harassment, cyberstalking, and exploitation, calling for enhanced safety measures that do not hinder user convenience.
- promote and call for women and youth leadership in tech policy and cybersecurity decision-making, particularly ensuring gender-sensitive approaches.

- advocate for secure access to digital tools and services for women and youth in rural and marginalised communities.
- can set up and facilitate safe spaces or platforms for the victims to discuss their experience, seek suggestions, and find emotional support.
- form peer groups that can help in combating bullying and harassment cases, both online and offline.
- can come up with petitions and rallies against any platform or policy that fails to serve their promised responsibilities.

Understanding Information Disorders

The advent of social technology in this digital age promised us a connected and collaborative community, with the world coming closer to a 'global village'. With it came information pollution, rising on a global scale. While the digital age promises instant access to information at the tip of a finger, this ideal is often disrupted by what is termed as 'information disorder'. This umbrella term covers the spread of misinformation, disinformation, and malinformation. While misinformation refers to false information shared without harmful intent, disinformation involves deliberate attempts to mislead. Malinformation, however, involves sharing true information with the intent to harm. A particular challenge arises when truth is manipulated-presenting partial facts or context in a way that makes the narrative seem credible. This blend of truth and falsehood creates confusion and erodes trust in digital spaces, indicating how information can be misleading even when it contains elements of truth. By presenting facts in a distorted or out-of-context manner, partial truths are used to create a narrative that appears credible, making it harder for the reader to recognise the manipulation. The mix of truth and falsehood makes the entire story believable, even though key details may be omitted or misrepresented, ultimately misleading the audience without outright lying. This exploitation of truth creates confusion and erodes trust in information.

Information Disorder

Information disorder encapsulates all the ways in which the information in the ecosystem is polluted. Falsifying facts, manipulating information, disseminating information without considering the repercussions, demeaning the faiths and beliefs of others, and supporting propaganda and fake news with or without a personal stake is termed information disorder.

In their initial research and publication, Claire Wardle and Hossein Derakhshan distinguished three categories of information disorders: a) disinformation, b) misinformation, and c) malinformation.[51]

Disinformation	False information being shared knowingly to cause harm
Misinformation	Inaccurate information is being spread without any malicious intent.
Malinformation	Sharing true information to cause harm, commonly by revealing private information to the public.

Forms of Information Disorder:[52]

1. *Fabricated content:* Completely false content created to deceive and cause harm, such as deepfakes. Distinguishing between the real and fabricated content is extremely difficult to the naked eye. If you have seen any "deepfakes" that can often be categorised as "fabricated content," you know how deeply it impacts our trust in the messages we see. *Example:* fake videos of public figures making false statements.
2. *Manipulated content:* when authentic data or visuals are altered with the intention to mislead. Typically, this involves manipulating photos and videos to make them appear realistic, but the original message of the authentic content is altered. *Example:* a protest image digitally altered to include offensive signs.
3. *False context:* when authentic content is spread with inaccurate or misleading context. An example would be a picture reshared to align with a different storyline. It is a potent type of misinformation, utilising authentic content that cannot be refuted but is manipulated in a harmful manner to promote a specific argument. *Example:* an old flood photo shared on social media as recent disaster evidence.
4. *Imposter content:* when authentic sources are copied. This type of misinformation capitalises on the confidence you might have in a particular entity, like an organisation, individual, or company. Numerous phishing and smishing (phishing via messages on mobile phones) attacks are crafted in this manner: using the logo or name of a famous brand to make it seem like you

[51] https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

[52] https://commonslibrary.org/disinformation-and-7-common-forms-of-information-disorder/

are receiving legitimate content. Being distracted or in a rush is sufficient to occasionally become prey to manipulation. *Example:* fake bank emails requesting sensitive information.

5. *Misleading content:* using information in a misleading way to portray a situation or person. It involves selecting specific photos, quotes, or statistics to back up a point. Detecting this type of altered content is challenging without the necessary expertise, investigation, and verification of sources. *Example:* highlighting only data that supports a biased argument.
6. False connection: when the headlines, visuals, or captions do not align with the content. While false connections like clickbait headlines may seem harmless and merely annoying at first, they can actually damage trust in media and fuel polarisation on a broader scale. *Example:* headline claiming a celebrity's death on social media to attract readers
7. Propaganda: Propaganda is when information is spread to support a specific cause or perspective in order to persuade a certain mindset, reaction, or behaviour. Individuals have employed propaganda to promote beneficial behaviours like rationing and joining the military in the world wars, as well as to promote increased seatbelt usage and decreased smoking in recent times. *Example:* coordinated fake accounts spreading biased narratives during elections
8. Satire or Parody: while these are comedic, satire and parody can also be used to intentionally promote rumours and conspiracies, and if accused of wrongdoing, they may not be taken seriously or literally and receive minimal consequences. This type of misinformation can quickly be passed on or altered, moving away from its original, comedic setting.
9. Error: mistakes represent a type of false information. They are completely accidental but result in damage and confusion in the information environment. Respected news outlets usually rectify their mistakes; however, by then, the impact is already apparent. Typically, there is a gap between when the initial report is made and when the retraction is issued. There is enough time for the error to propagate, and only a subset of individuals who were given the wrong information will get the correction.

Combating Information Disorder and Tools for Verification

Information disorder has a lasting impact on our society and democracy as it erodes trust, polarises communities, and undermines informed decision-making. People need the right skills to effectively tackle this challenge. The United Nations Educational,

Scientific, and Cultural Organisation (UNESCO) uses the term 'Media and Information Literacy' to describe the skills that help us access, understand, evaluate, and responsibly share information[53]. Women and youth-led Civil Society Organisations (CSOs) are crucial in addressing information disorder by actively engaging in verification, helping ensure digital spaces remain credible and trustworthy.

Verification is the process of ensuring the accuracy and authenticity of information before it is shared or disseminated. In the context of digital media, it involves checking sources, cross-referencing claims, and validating visual and textual content to prevent the spread of misinformation. Below are some tricks to verify the information.

Verifying fake websites or social media accounts involves:

For websites:

- Look for misspellings or extra characters (e.g., "amzon.com" instead of "amazon.com").
- Ensure the website uses HTTPS (secure connection), indicated by a padlock icon in the browser's address bar.
- Verify the domain extension (eg, .com, .org, .gov, etc). Official sites often use specific extensions.
- Look for poor grammar, typos, or unprofessional design.
- Check if links work properly. Fake sites often have broken links or redirect to unrelated pages.
- Legitimate sites usually have clear contact details like an address, phone number, or support email.
- Test the contact details if you're unsure (e.g., call the listed number).
- Fake websites often misuse the logos of known organisations. Verify partnerships through the official organisation's site.

For social media accounts:

- Many platforms (e.g., Twitter, Instagram, Facebook) use verification badges (blue checks) for official accounts. Platforms like Facebook, Instagram, and Twitter have options to report fake accounts.
- Check the account creation date: Fake accounts are often newly created.
- Examine the content: Are posts consistent with the brand or person? Is there suspicious or generic content?

[53] UNESCO, Media and Information Literacy, accessed at: https://en.unesco.org/themes/media-andinformation-literacy

- Look for unusually high follower counts with low engagement (a sign of fake followers).
- Beware of minor changes (e.g., "Brand_Official" vs. "Brand0fficial").
- Check the comments: Fake accounts often use bots to spam generic comments. Real accounts have meaningful interactions with followers.
- Use the official website of the brand/person to find their legitimate social media links.
- Search for announcements or clarifications about fake accounts from the official account.
- Fake sites or accounts often approach users with offers, giveaways, or threats.
- Hover over links to check their destination before clicking.
- Anti-phishing software or browser extensions can help detect suspicious sites/accounts.

Verifying the content's authenticity:

- Before relying on or believing any information/news, check the content. Is the content from a well-known, credible organisation or individual? Trusted domains include.edu, .gov, or major media outlets.
- Check if the author/organisation is well-known for their expertise in the topic. It is highly important to look for credentials or affiliations.
- Be cautious of spoofed or similar-sounding URLs
- Verify facts by comparing the content with other reliable sources.
- Poor grammar, spelling errors, or overly sensational language may indicate unreliable content.
- Check if the content is overly one-sided or propagating a specific agenda.
- Are claims supported with credible references, links, or data?
- Is the information current and relevant? Outdated content may no longer be accurate.
- Check for timestamps or updates.
- Join reputable forums or communities discussing the topic.

Further, CSOs can also

- actively run campaigns to educate communities on identifying and combating misinformation
- train individuals to recognise altered or misleading images
- amplify the voices of marginalised communities, ensuring their stories remain factual and free from manipulation

Digital Inclusion in Policy Development

Krishaank Jugiani and Bijaya Roy
Senior Research Associates

Overview of the Module

In this module, participants will gain a crucial understanding of key concepts and practical strategies for effective engagement in policy-making. The course will emphasise the importance of diversity, ensuring that contesting perspectives and experiences are represented in policy discussions. Participants will explore intersectionality to understand how overlapping social identities affect access to digital resources and policy impact.

The course will also discuss the importance of consultations in the advocacy process, emphasising the need to gather insights from a broad range of stakeholders and to ensure that marginalised voices are included in decision-making forums. It will also focus on conversation around how these laws often fail to be inclusive of women, youth, and minority communities, with an exercise for participants to identify ways to make the laws more inclusive.

Community engagement strategies will be discussed to foster collaborative efforts and create meaningful interventions. Practical tips will include developing inclusive consultation processes, leveraging diverse community networks, and creating platforms for ongoing dialogue. By engaging with each other, different groups can amplify their voices and drive impactful policy changes that advance digital inclusion and equity.

What is digital inclusion?

Digital inclusion is defined as "equitable, meaningful, and safe access to use, lead, and design of digital technologies, services, and associated opportunities for everyone, everywhere".[54]

Digital inclusion is all about addressing barriers to accessing and using digital technologies, based on intersectional, human rights-based policies and multi-

[54] https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf

stakeholder actions. It also aims to ensure that consumers' online human rights are protected and to promote equitable opportunities for all, particularly marginalised communities. This involves addressing structural inequalities, ensuring affordable access to the internet, devices, and digital skills, and fostering safe, inclusive online spaces free from discrimination. Inclusion also requires involving diverse groups in designing and evaluating digital policies and technologies to ensure no one is left behind.

Factors that influence digital inclusion

It has been observed that overlapping social identities, such as **gender, socioeconomic status, disability, and ethnicity**, create **intersectional disadvantages** that shape individuals' access (or lack thereof) to digital resources and determine the impact of policies on different groups. A policy may affect individuals differently based on the interaction between their identities, causing **uneven access to opportunities, information, and services**. For example, during public health emergencies, governments and organisations disseminate information about services through digital channels like social media. Marginalised communities like women in rural areas, with lower internet access rates, may miss critical updates, while LGBTQIA+ individuals may struggle to access health services tailored to their needs due to a lack of inclusivity in outreach strategies.

A study found that socially vulnerable groups encounter significant challenges such as limited digital access, low digital competencies such as information and data literacy, communication and collaboration, digital content creation, safety, and problem-solving, and a lack of knowledge to meaningfully use digital media, which exacerbates their marginalisation and deepens existing inequalities. It also emphasised that the social structures, including education, income, and social status, play a crucial role in influencing individuals' ability to leverage digital tools for empowerment and social inclusion

For example, individuals with higher levels of education and income are more likely to use the internet to expand their professional networks, access online learning platforms, and find better job opportunities. Even if a person has a mobile phone but does not know how to operate it (i.e. does not have access to the desired skill set), it will be of limited use.

Some of the key factors that contribute to the **differentiated impact of digital policies** and access to digital resources are mentioned below.

Factors	Group Affected	How do these factors result in digital exclusion
Gender identities	Female and transgender individuals	The restrictions stem from historical inequalities in gender, preventing these groups from accessing education and economic resources, thus making them limited in accessing and benefit from the digital policies.
Socio-cultural identities	Ethnic and religious minorities	Systemic discrimination, lack of representation, and cultural biases also exclude them from policymaking processes and reduce their access to resources.
Geographical Identities	Residents of villages and small towns, in remote locations	Geographic isolation results in underdeveloped infrastructure, fewer initiatives in digital literacy, and less investment in technology, leaving them disconnected.
Socio-economic conditions	Migrant communities, low-income households, rural and urban poor	Due to poverty or socio-economic instability, they cannot afford the digital equipment and access to the Internet; training is also a challenge for them. Hence, they keep relying on other people for digital access and are prone to exclusion.
Disabilities	People with physical, cognitive, or sensory disabilities	Poor inclusive design and assistive technologies often result in the exclusion of people with disabilities
Profession	Journalists, human rights defenders (HRDs)	In a few professions, individual's activities are often against power structures, hence exposing them to cyberattacks, snooping and systemic restrictions on digital freedom.

Challenges faced by marginalised groups

Women

- Women face limited access to digital resources due to socio-cultural norms, financial constraints, and gender-based discrimination.

  For example, women are less likely to own smartphones or have internet access in South Asia, impacting their ability to participate in policy discussions. However, even if women have limited access to technologies and digital resources, policies around these shape societal systems that affect them, such as digital ID systems for accessing welfare or online banking for financial inclusion. Similarly, women without access to a smartphone may still need to interact with digital platforms via intermediaries (family members, friends or local cyber cafes) for services like government benefits or healthcare, making them vulnerable to exploitation or exclusion. Thus, it becomes necessary to advocate for inclusive policies that consider issues of women directly and indirectly accessing these services, along with helping them bridge this digital divide through skill-building programmes, and collaborating with NGOs to provide women with devices and digital resources.

- Limited Representation in Policy Roles: There is a lack of female representation in policy-making, technology, and decision-making positions, which limits their voice and influence in the digital policy landscape.
- Gender-Based digital violence: Women face disproportionate online abuse, impacting their personal, professional, and mental well-being. Studies show 73 percent of female journalists have experienced online violence. A study by the Bangladesh Legal Aid Services Trust (BLAST) revealed that 73 percent of women in Bangladesh using the internet have experienced cybercrime, while research by the international organisation Article 19 found that 70 percent of online harassment victims are women aged between 15 and 25.
  - Abuse takes various forms, including hate speech, trolling, astroturfing, cyberbullying, doxxing, and deep-fakes.
  - Harassment often includes sexist slurs, threats of violence, non-consensual sharing of personal photos, and sexually explicit deep-fakes.

Ethnic and Linguistic Minorities

- Language Barriers: Digital policy content and consultations are often conducted in mainstream languages, including English, which marginalises those who speak

regional or minority languages, affecting their ability to understand and engage with policy discussions.

- Cultural Exclusion: Ethnic minorities frequently face discrimination in digital spaces and may find their cultural needs overlooked in policies, leading to policies that are not culturally inclusive, sensitive or representative.

Example: Digital violence targeted at minorities

The Sulli Deals and Bulli Bai cases exemplified hate speech through coordinated efforts aimed at harassing women journalists and activists from a specific minority religious community. These women were portrayed as "deals of the day" in online mock auctions via apps hosted on the GitHub platform.

Youth

- Barriers to Digital Literacy: Many young people, especially in rural areas or marginalised communities, lack the digital literacy necessary to engage meaningfully in digital policy. Access to high-quality digital education is still limited, especially for youth from low-income families.
- Policy Marginalisation: Youth, especially teenagers and tweens' voices, are often excluded or underrepresented in policymaking processes, leading to policies that don't always address their unique needs or experiences with digital spaces.
- For example, policies like parental consent requirements and banning of tracking or behavioural monitoring when they are using digital services. Parental consent policies often exclude youth perspectives, assuming parents are the best decision-makers, which can restrict access for teenagers, particularly in households with limited digital literacy or socio-cultural barriers. Similarly, debates around banning behavioural monitoring and targeted advertising, aimed at them, overlook the nuanced needs of youth, who may value personalised content, but these debates tend to focus on privacy risks or parental control only.

LGBTQIA+ Community

- Discrimination and Safety Concerns: LGBTQIA+ individuals often face discrimination, harassment, and targeted attacks in online spaces, making it unsafe for them. Fear of backlash even deters many from participating openly in digital advocacy and policy discussions.
- Lack of Inclusive Policies: Policies in many South Asian countries do not explicitly address the challenges faced by LGBTQIA+ individuals, such as lack of access to safe digital spaces, privacy concerns and cyberbullying, leading to a lack of protections in the digital space.

Examples of harassment faced by LGBTQ+ individuals

LGBTQ+ individuals also face pervasive online harassment characterised by sexual propositions, blackmail, and extreme threats from religious extremists, which creates a hostile environment for identity exploration. At times, users feel unsafe disclosing their identities due to trauma and anxiety, leading them to create multiple fake accounts for anonymity, which complicates self-expression and fosters feelings of alienation.

In a study on LGBTQ+ social media users, out of 31 participants, 11 reported shifting from public to private online groups, pages, or communities to ensure safer and more secure participation. However, this transition poses difficulties for many LGBTQ+ users, as these private spaces are often very difficult to locate.

Rural and Low-Income Populations

- Inadequate Access to Digital Infrastructure: Rural areas face challenges like poor internet connectivity and a lack of digital infrastructure, preventing these populations from actively using digital services and also participating in digital policymaking.
- Economic Constraints: High data costs and a lack of affordable digital devices limit engagement for low-income populations, making it difficult for them to be involved in policy processes or to access digital resources fully.

  Examples: A study highlighted that there is a significant digital divide between economic classes in India- among the poorest 20 percent of households, only 2.7 percent have access to a computer, and 8.9 percent have internet access. In contrast, for the wealthiest 20 percent, these figures rise to 27.6 percent and 50.5 percent, respectively.

Persons with Disabilities

- Accessibility Barriers: Most digital platforms and public consultations on policy are not accessible for individuals with disabilities. Inadequate accessibility features, such as the absence of screen readers or closed captioning, prevent their effective participation in the digital ecosystem.
- Lack of Representation: There is limited representation of persons with disabilities in digital policymaking processes, which results in policies that fail to accommodate their needs, perpetuating digital exclusion.

Example: according to a study in 2021, in India, there was a 19 percent mobile disability gap (differences between persons with and without disabilities) in ownership and use of mobile phones and 32 percent for mobile internet usage.

How to identify whether a law/policy is inclusive or not?

To identify whether laws are inclusive or not, look for the following things-

- Which stakeholders could be impacted by a policy or law?

Example: In a policy on digital education, check whether it includes considerations for rural and underprivileged communities' access to devices and the internet, ensures platforms are accessible to students with disabilities, incorporates teacher training for equitable delivery, provides provisions for gender equality and protection against online harassment, and addresses issues of affordability and language diversity.

- Who contributed to the formulation of the policies/laws?

How to check: Review the process of policy formulation to see whether public consultations or invitations for comments were organised. Examine records to identify who participated, whether the consultations included representatives from marginalised communities, gender groups, or experts in social inclusion. For example, were women's organisations part of the process or not?

- Has the policy/law considered its implications on different groups?

How to check: Analyse whether a Regulatory Impact Assessment[55] was conducted to analyse how the policy would affect various demographic groups.

- What will be its impact on equality among different groups?

How to access: Examine whether the law/policy has provisions to create opportunities to reduce gaps in access, representation, and outcomes and includes safeguards against discrimination between advantaged and disadvantaged groups. Whether it has provisions that aim to enable equitable participation in policy implementation.

- What is the monitoring and evaluation mechanism under those policies/laws?

How to do: Check if the policy has mechanisms for tracking implementation and assessing impact over time and across groups, whether it includes measurable goals

[55] Regulatory Impact Assessment (RIA) - CUTS CCIER

and targets to evaluate progress. include provisions for third-party or independent audits to assess the policy's performance objectively, etc.

- Does the policy/law make any group more susceptible to online abuse, cybercrime, digital divide?

Try to identify the potential unintended consequences of that policy.
Example: A policy mandating online verification for access to social services without addressing the digital divide could exclude rural communities or people with limited digital literacy.

What are the key concepts for effective engagement in advocacy?

What is advocacy?

Advocacy can be defined as public support for or recommendation of a particular cause or policy. Essentially, it is a political process undertaken by individuals or groups to influence decisions within political, economic, and social systems and institutions. In this module, however, we will discuss advocacy with a particular emphasis on the inclusion of women and youth.

Objectives and aims of advocacy

1. Promote specific causes or ideas, often involving interests of different communities and promoting policies that are inclusive, gender-sensitive and evidence-based to ensure fair representation of marginalised identities.
2. Raising public awareness, including among rights groups, for influencing government decisions, and pushing for laws and regulations that serve the broader public good, especially underrepresented groups.
3. Identifying and building relationships with stakeholders and decision-makers, and with media to amplify inclusive narratives, and mobilising public support to push policy narrative around the rights of women, marginalised communities, and other vulnerable groups.

Advocacy includes a variety of activities, such as research, public education, and grassroots mobilisation and aims to change public opinion and create a movement around inclusive, socially equitable issues. In the space of digital policymaking, advocacy will aim to address the above-discussed issues, such as lack of digital access,

online violence, harassment, cyberbullying, etc., and ensure that the policies are intersectional, among others.

Intersectionality in advocacy

Intersectionality means the interconnectedness of social categories like caste, class, ethnicity and gender, which create overlapping systems of discrimination or disadvantage for individuals or groups. Intersectionality in advocacy, particularly within tech policy, emphasises the interconnected nature of various social categorisations such as race, gender, and class, and how these intersections affect individuals' experiences and access to technology. *For example,* the use of AI raises significant concerns about biases, such as in facial recognition technologies. This can disproportionately impact minority and lower-class women. This is because AI systems trained on data sets that lack diversity or reflect existing social inequalities may misidentify individuals from marginalised communities.[56]

Why is intersectionality important for advocacy?

- To ensure that the diverse experiences and needs of everyone are considered and no one is left behind.
- Identify and advocate for addressing issues like unequal access to technology, digital exclusion and algorithmic bias.

What are the key things to consider in Intersectionality and Advocacy of Tech Policy?

1. Advocacy must tackle the complex relationship between technology, democracy, and human rights. Technology can enhance democratic processes by improving access to information and enabling citizen engagement, but it can also threaten human rights through surveillance and misinformation. The impact of technology depends on its use and regulation, making effective governance essential to ensure it promotes democratic values and protects human rights. This also includes recognising how marginalised communities are disproportionately affected by tech policies or their enforcement. For example, during protests or political/social unrest, governments often impose internet shutdowns, disproportionately affecting people and communities that rely on digital connectivity for access to education, healthcare, and livelihoods.[57]

---

56 How AI reduces the world to stereotypes

57 "No Internet Means No Work, No Pay, No Food": Internet Shutdowns Deny Access to Basic Rights in "Digital India" | HRW

2. The Role of Emerging Technologies: Emerging technologies can both empower and cause harm. For instance, while AI can enhance decision-making, it may also perpetuate biases if not carefully regulated. *(Discussed in detail in module 2)*

3. Interdisciplinary Approaches: Effective advocacy requires integration of multiple approaches- social, political, economic, legal, etc. It also requires collaboration across sectors-government, academia, civil society, and industry- to address multifaceted issues. This can be done by bringing together experts from diverse fields in policy discussions to tackle complex technology policy issues.

4. Ethical Considerations: Advocacy must prioritise ethical frameworks that consider the societal implications of technology. This includes addressing issues like data security, privacy, transparency, algorithmic bias, etc., which disproportionately impact vulnerable populations. For example, one of the ways by which privacy of the individuals is ensured is by incorporating privacy-by-design features in the technologies and tech policies that advocate for such features. In this way, privacy-by-design can serve as an ethical framework for new and emerging technologies.

5. Empowering Voices: It's crucial to amplify the voices of those most affected by tech policies. Advocacy should focus on inclusivity to ensure that diverse perspectives inform policy decisions. This can be done by creating and/or supporting platforms where marginalised communities can voice their concerns, and partnering with civil society organisations and community leaders to ensure that the most affected populations are not only heard but also actively engaged in policy advocacy.

6. Need for Continuous Learning: Advocates must remain adaptable and informed about rapidly evolving technologies and their implications for society.

Principles of advocacy in digital policy

There are different principles of advocacy, like transparency, participation, accountability, and equity in digital policymaking. These concepts are explained below.

Accessibility and Equity: Advocacy processes must be equitably accessible and represent the voices of everyone, regardless of ability, location, race, gender identity, sexual orientation, or economic status. This also includes data, tools, skills, and opportunities for all. Advocacy should emphasise policies that promote inclusivity and fairness, allowing all individuals to benefit from digital products and services. Example: Digital literacy campaigns tailored for the rural population, especially women in low-income communities, where training materials can be translated into local languages

and delivered through workshops. An example of such an initiative is CUTS' capacity-building workshops on cybersecurity conducted for women entrepreneurs in West Bengal. These workshops were delivered in regional languages, ensuring that complex topics like online safety were accessible and easily understood by the participants, fostering greater digital awareness and inclusion.

To ensure accessibility and equity advocacy for digital policies

- identify gaps in access to technology within your community, such as a lack of broadband or digital skills.
- advocate for equitable access policies, such as subsidies for internet connectivity or free public Wi-Fi zones.
- partner with local NGOs to develop digital skill-building programmes for such groups.

Transparency: Advocacy processes must be handled with full transparency, ensuring that the concerns and recommendations of the stakeholders are in the public domain. Advocacy efforts should also mention clear and open communication regarding how data is collected, used, and shared, and ensure organisations remain transparent about their security measures. For example, CSOs, NGOs and community leaders can track how government funds for digital infrastructure projects are allocated and spent, ensuring that the benefits reach intended beneficiaries. They can also

- engage in public consultations and demand clarity on how data is collected, stored, and used by companies or government agencies.
- advocate for mandatory disclosures by tech companies about their security practices and algorithmic decision-making.

Participation: Advocacy in digital policy must foster broad stakeholder participation, encouraging the involvement of marginalised and vulnerable communities. This includes consulting a diverse range of voices, ensuring that policy decisions reflect the needs and perspectives of all individuals, particularly those often excluded from decision-making processes. Example, Participating in, and if possible, organising stakeholder consultations to put forth views of different communities to incorporate their perspectives into digital and tech policies. They can also

- create forums or surveys to collect feedback from underrepresented voices and present it to policymakers.
- join or establish advocacy groups to amplify the concerns of excluded communities.

Accountability: Organisations and policymakers should be held accountable for their conduct in the advocacy process. Advocacy should promote mechanisms that hold digital actors accountable for data protection, ethical practices, and combating harmful practices like misinformation, bias, and cyberbullying. For example, seeking accountability from government bodies that use technologies in providing welfare services to people.

- monitor and report unethical practices by organisations, such as misuse of personal data or lack of cybersecurity measures.
- use tools like Request to Information to demand information from public institutions on digital policy initiatives.
- advocate for clear grievance mechanisms for victims of cyberbullying, fraud, or algorithmic harm.

Ethics and Responsibility: Advocacy should prioritise ethical standards in digital policymaking, ensuring that products, services, and platforms respect data privacy, eliminate algorithmic bias, and reduce negative societal impacts. Policies should aim to foster responsible technology use and ensure that technologies contribute positively to society. For this,

- engage with policymakers to advocate for ethical tech guidelines and their enforcement through legal frameworks.
- conduct community workshops to educate people about their digital rights, including data privacy and ethical technology use.
- partner with academia and tech companies to co-develop frameworks for reducing algorithmic bias and ensuring ethical practices.

It is important to note that for a good effective advocacy, which considers these principles, evidence gathering is important.

Why and how to gather evidence for digital policy advocacy?

Gathering information for advocacy is essential because it ensures your efforts are evidence-based, targeted, and impactful. *For instance, you observed that the lack of safe and inclusive online environments for LGBTQ+ users on social platforms in your country is an issue and decided to advocate for inclusive online spaces for LGBTQ+ users.*

To start with the advocacy, you should do a comprehensive study. By conducting a comprehensive study, you can:

1. **Understand Challenges:** Analyse the impact group's experiences on social platforms to identify specific issues like harassment or exclusion.
2. **Identify Gaps:** Examine platform policies and domestic regulations to uncover shortcomings in safety measures or inclusivity.
3. **Strengthen Credibility:** Use data-driven insights to build a persuasive case for policy changes.
4. **Propose Solutions:** Recommend practical measures, such as enhanced reporting systems or inclusive content moderation practices.
5. **Benchmark Standards:** Align with international best practices to push for globally recognised policies.
6. **Support Change:** Provide actionable insights to engage stakeholders and drive long-term improvements.

What is the data collection process for advocacy on Digital Rights?

a. Choose a Focus Area

- Identify a policy or aspect related to digital rights that requires attention, investigation or policy change (e.g., data privacy, online harassment, digital inclusion).

  Example: *digital divide faced by the LGBTQ+ community as compared to the general population.*

b. Determine Criteria for Research and Data Gathering

- Outline the specific criteria or key information to collect.
  - Start by identifying the target group. This includes people/groups directly/indirectly impacted due to a particular issue.
  - Clearly articulate the purpose of your research (eg. to understand the level of digital access among LGBTQ+ people);
  - Identify the data types and sources (eg. quantitative data on internet penetration rates, smartphone ownership statistics, while qualitative data can be gathered from interviews with LGBTQ+ people or focus groups to gather lived experiences with digital tools)
  - You can also define specific indicators (such as access to technology, digital literacy, etc)

c. Collect relevant data

- Gather as much relevant data as possible through both secondary sources (such as websites) and discussions with impacted groups or victims.

- Explore academic journals, government reports, and industry publications.
- Use intergovernmental reports, like those from the United Nations, SAARC, etc.
- Gather qualitative data through interviews or surveys. Surveys could be both quantitative and qualitative, based on the objective and scope.
- Explore Reports of Civil Society Organisation and Academics, Tech Industry reports/insights, etc.

- Collect case studies/examples where the policies failed to address a concern or created a challenge for stakeholders.
- Seek recommendations from stakeholders to address the concerns they would highlight.

  For instance, in addition to digital access, stakeholders can highlight that LGBTQ+ individuals face structural barriers, such as income disparities, discrimination, and harassment in digital spaces, limited access to online resources that support their well-being, etc.

How to implement advocacy?

A. Use findings as a Tool for Advocacy

- Develop an advocacy toolkit[58] to summarise your findings concisely.
- Leverage social media and blog posts to share the fact sheet and raise awareness.
- Prepare policy briefs based on findings and share with relevant government departments and private stakeholders for implementation.

B. Engage with other advocacy groups

- Identify organisations and leaders actively engaged in both research and advocacy of digital rights.
- Regularly engage with them by setting up consistent meetings through multiple engagement channels (e.g., in-person, online, and over the phone), share updates and seek feedback. It will help ensure that their concerns are continuously heard and addressed, and also create a sense of inclusion and empowerment, allowing them to actively shape policies that affect their digital rights and well-being.

A list of few organisations working in this space from different countries are, such as Just Net Coalition, IT for Change (India); Voice for Interactive choice & empowerment (VOICE), Internet Society Bangladesh Chapter (Bangladesh); Digital

[58] Digital Advocacy Toolkit | Pollicy, A Responsible Tech Advocacy Toolkit | by Tim Frick | B The Change

freedom Coalition, Open Internet (Nepal); Hashtag Generation, LIRNEasia (Sri Lanka).

C. Identify the relevant government agencies and policymakers

Government agencies are responsible for drafting, reviewing, and implementing laws and regulations that directly affect the tech sector, prioritising political, social, and economic goals, making them crucial stakeholders for advocates. Therefore, for targeted advocacy, it is important to identify relevant government agencies, understand their structure as well as their responsibilities.

Understanding the Government Structure: Government agencies operate at different levels—federal, state, and local—each with specific responsibilities and jurisdictions.

Main Institutions: At the federal and state/provincial levels, key institutions include the executive, legislative, and judicial branches.

Relevant federal government agencies and policymakers

- **India**: Parliamentary Standing Committees, Ministry of Electronics and Information Technology (MeitY), Telecom Regulatory Authority of India (TRAI), *upcoming* Data Protection Board under DPDP Act
- **Bangladesh**: Ministry of Posts, Telecommunications, and IT (MPTIT), Bangladesh Telecommunication Regulatory Commission (BTRC), Information and Communication Technology (ICT) Division
- **Nepal**: Ministry of Communication and Information Technology (MoCIT), Nepal Telecommunications Authority (NTA), National Planning Commission (NPC
- **Sri Lanka**: Ministry of Technology, Telecommunication Regulatory Commission of Sri Lanka (TRCSL), ICT Agency of Sri Lanka (ICTA)

These bodies, like telecom authorities and data protection agencies, play crucial roles in shaping and enforcing digital policies. For instance, TRAI (India) and BTRC (Bangladesh) manage telecom licences, along with dedicated consumer affairs departments.

Furthermore, some federal-level institutions provide digitally-enabled services to citizens too. For example, Aadhaar's digital infrastructure, including the Aadhaar-enabled Payment System (AePS), has facilitated doorstep banking services in remote

areas, allowing individuals to withdraw cash, transfer funds, and conduct other basic transactions using only their Aadhaar number.[59]

State Agencies: Each state has its own agencies responsible for various sectors such as health, education, and transportation, supported by dedicated IT departments. These government agencies collect extensive data and offer digitally enabled services to citizens, streamlining governance and enhancing service delivery.

Local Agencies: Local governments also have agencies that manage community services, zoning, and public safety.

How to Identify Relevant Government Agencies and Policymakers

- Government Departments and Ministries:
  - Research the relevant ministries and their sub-departments based on your area of interest (e.g. Ministry of Electronics and Information Technology, Ministry of Information and Broadcasting, etc.)
  - Explore organisational charts on their websites to identify divisions and key officials handling specific portfolios.
  - Review their annual reports and press releases to understand their priorities and the officials responsible for implementing them.

- Regulatory Bodies:
  - Identify sector-specific regulatory bodies, such as the Telecom Regulatory Authority of India (TRAI) for telecommunications
  - Visit their official websites to explore their mandates, leadership, ongoing consultations, and recent initiatives.
  - Check for contact details and schedules for public consultations, as these are opportunities to directly engage with regulators.

- Government Websites: Start with official government websites for a list of agencies and their functions.

  India: Visit websites of ministries and departments like the Ministry of Electronics and Information Technology in India. Visit websites like **MyGov** (www.mygov.in), launched by the Government of India to encourage citizen engagement in governance. It allows people to share ideas, participate in discussions, and

[59] Aadhaar: A Unique Identity For The People.

contribute to decision-making processes on various government initiatives and policies.

Sri Lanka: Visit Sri Lanka's ePaticipation Portal under the Information and Communication Technology Agency (ICTA) facilitates citizen engagement. It allows citizens to provide input on government policies and participate in decision-making processes.

Nepal: *e-Government Portal* allows citizens to access services like grievance redressal and participation in public policy discussions.

Bangladesh: Bangladesh does not have a centralised platform for public consultations, but relevant information can be found on specific government ministry websites. The Ministry of Foreign Affairs (MOFA) (mofa.portal.gov.bd) provides updates on foreign office consultations, while the Ministry of Finance (MOF) (mof.gov.bd) shares details on policy amendments and related consultations.

- Legislative Directories: Use directories or portals that list members of parliament, members of parliamentary standing committees and other legislators.
- News and Publications: Read news articles, government publications, and reports to understand which policymakers are influential in your area of interest.
- Advocacy Networks: Join advocacy groups and professional associations that are already engaged in policy work. These networks often have insights and connections with key policymakers.
- Public Records: Access public records and databases to find detailed information about specific policymakers and their roles.

How to Connect with Policymakers

- Contact Information: Gather contact details from government websites, including email addresses, phone numbers, and office addresses.
- Formal Letters and Emails: Write formal letters or emails explaining your cause, why it matters, and requesting a meeting or discussion.
- Social Media: Follow and engage with policymakers on social media platforms like Twitter and LinkedIn. They often share updates and insights, and you can use these platforms to start conversations.
- Public Events and Town Halls: Attend public events, town halls, and forums where policymakers are present. These events are great opportunities to connect in person.

- Lobbying and Advocacy Groups: Partner with lobbying and advocacy groups that have established relationships with policymakers. They can provide introductions and support.
- Petitions and Campaigns: Organise or participate in petitions and campaigns that draw attention to your cause. This can create a collective voice that is harder to ignore.

D. Suggestions to undertake an inclusive and meaningful consultative process

- Target stakeholders from varied backgrounds, including community leaders, NGOs, youth organisations, legal experts, and policymakers. Building a wide network is critical for a holistic understanding of community needs and perspectives.
- Engagements could include informal gatherings, workshops, and focus group discussions to establish a baseline of trust and communication in collaborative environments. Create shared goals and establish clear, open channels of communication.
- Collaborative online platforms (such as Slack, Google Workspace, or specialised community software) can help streamline document sharing, project planning, and cross-collaboration, fostering transparency and consistent stakeholder engagement.
- Consult with lawyers and legal advocates to navigate compliance and regulatory challenges effectively. Legal professionals can provide insights into local laws that may affect policy recommendations, ensuring consultations are both impactful and compliant with current legal frameworks.
- Involve and collaborate with experts, think tanks, civil society organisations, academia, and industry leaders, as these stakeholders bring valuable perspectives on the technical, economic, and practical implications of policies and help enhance the effectiveness and depth of policy recommendations.

How to engage with stakeholders?
• Identify key contacts and potential partners: Look for organisations already active in digital rights and community support, as they can provide both expertise and an established network. • Organise collaborative workshops and knowledge sharing sessions to collectively brainstorm solutions. These sessions can become a platform for legal professionals and community leaders to share insights and build a unified advocacy message.

How to engage with stakeholders?
● Keep stakeholders informed about consultation and policy developments. A continuous feedback loop with stakeholders strengthens trust and demonstrates that their contributions are valued and acted upon.

E. Best practices and techniques for undertaking consultations with diverse communities

- Allocate ample time for engagement to ensure each community's views, concerns and demands are represented. This is critical in countries with complex cultural or linguistic diversity.
- Research cultural norms and context, and acknowledge community-specific norms, values, and languages when designing consultations. For example, in South Asian contexts, gender roles and socioeconomic status can influence perspectives on technology and access to digital resources. Tailoring engagement strategies to these cultural factors can increase inclusivity.
- Use accessible language and ensure that all materials are easy to understand. For multilingual communities, offering translations or community interpreters can make consultations more accessible and meaningful.
- Diversify engagement channels and provide means for participation, such as in-person gatherings, online discussions, and surveys. Use different channels to communicate with stakeholders, including people with disabilities, rural populations, and groups with limited internet access.
- Anonymise the views and opinions of stakeholders, especially when they deal with sensitive matters.

F. Strategies for approaching, communicating and engaging relevant policymakers to centre the voice of women and youth

- Highlight specific impacts on women and youth by using data, case studies, and personal stories to emphasise how policy decisions affect these groups uniquely. Data on digital inclusion, mobile internet access, or social media engagement among women and youth can add weight to arguments for inclusive policies.
- Form coalitions with organisations advocating for gender equity and youth inclusion. A unified front can present a stronger case and gain wider support, influencing policymakers more effectively.

- Arrange meetings or create briefing papers to present well-researched, concise briefs to policymakers. Clear, targeted communication, combined with a focus on solutions, can make these meetings impactful.

  Sample of a briefing paper on children's data protection

- Leverage traditional and social media: Use media channels to amplify marginalised voices. Share personal stories, success stories and perspectives on platforms like X, LinkedIn, and regional media outlets to broaden reach and rally public support.

Successful case studies of advocacies on digital rights

- **Case studies and successful advocacy campaigns**

Broadcasting Bill (India)[60]

The Broadcasting Bill in India, proposed to regulate content on television and radio, sparked advocacy efforts focused on maintaining freedom of expression and media independence. Organisations like the Media Foundation and Commonwealth Human Rights Initiative (CHRI), alongside journalists, pushed back against elements of the bill that appeared restrictive. Through public forums, campaigns, and media coverage, these advocates highlighted the risks of excessive government control over broadcast content. The bill faced resistance and has been withdrawn, showcasing that the efforts helped foster a broader discourse on media freedom in India and underscored the need for transparency in media regulation.

Right to Privacy as a Fundamental Right (India)[61]

In 2017, the Supreme Court of India, through a landmark ruling, affirmed privacy as a fundamental right, following a sustained advocacy campaign. Justice K S Puttaswamy played a pivotal role in this declaration of right to privacy as a fundamental right. Organisations like the Internet Freedom Foundation (IFF), Centre for Internet and Society (CIS), and Privacy International played crucial roles, emphasising the importance of privacy in an increasingly digital society. This ruling has since paved the way for strengthened data protection laws and inspired further advocacy around individual digital rights in India.

60 MIB Recalls 2024 Broadcasting Bill Copies After Backlash from Digital News Body and Opposition Parties .

61 Right to privacy inherently protected under fundamental freedoms in Constitution: Supreme Court - The Hindu

Examples of successful advocacy campaigns focused on digital rights of women, youth and other marginalised groups

1. The Youth For Women Foundation has established itself as a leader in promoting digital inclusion, reaching over 1,040 rural women and young people. Through a robust community-based digital literacy initiative, they have made strides in more than 20 rural communities, directly upskilling over 465 individuals. In addition to digital training, the Foundation has provided youth with leadership skills and resources, empowering them to launch 31 awareness campaigns. These initiatives have educated hundreds more on their digital rights, fostering both online and community-level change.

2. CUTS has been actively promoting cybersecurity awareness among women, youth, and SMEs across East and Northeast India, sensitising over 500 enterprises and 350 women through a cluster-based approach.[62] The initiative spans multiple states, offering workshops on securing online portals, conducting audits, and protecting critical infrastructure. Additionally, CUTS has also trained female journalists from South and Southeast Asia, including Bangladesh, India, Nepal, and Sri Lanka, to counter misinformation and conduct fact-checking, equipping them with essential digital tools.[63]

62 Cyber Safe East India – Workshops on Cyber Security for MSMEs and Women entrepreneurs, Phase I, II and III

63 Support For Women Journalists in Countering Misinformation & Disinformation in The Indo-Pacific Region, Phase I and II

For further information, refer to the below websites and readings:

1. Greater Internet Freedom,
2. Digital Rights School Curriculum - Greater Internet Freedom - Internews
3. Data Rights for Communities
4. Regulatory Impact Assessment (RIA) - CUTS ccier
5. Training Guidebook on Media Literacy (for media professionals in the Indo-Pacific Region)- CUTS
6. Digital Advocacy Toolkit | Pollicy
7. A Responsible Tech Advocacy Toolkit | by Tim Frick | B The Change
8. Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework | Universal Access in the Information Society
9. Loud Men Talking Loudly: Exclusionary Cultures of Internet Governance
10. Tackling issues at the intersection of technology, democracy, and human rights - Harvard Law School
11. Beyond Boundaries: Navigating Intersectionality in Tech & Beyond | by Women in Tech Society | Oct, 2024
12. What Are the Challenges and Triumphs of Intersectional Women in Tech?

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).