Introduction

This Blueprint is developed by the Freedom Online Coalition's (FOC) Task Force on Information Integrity (TFIIO), which is co-led by Denmark, the Netherlands, and the Wikimedia Foundation. This Blueprint is intended to be a guide to help navigate the challenges posed by the profound complexities of the online information ecosystem. Governments, industry, civil society, rightsholders, academics, citizens and other stakeholders all have profound interest in the technological and regulatory decisions that influence the future of information online. The Blueprint is articulated in three interconnected pillars – Agency, Trust and Inclusion –, which combined articulate a positive vision for a healthy online information ecosystem that supports the production and sharing of accurate, trustworthy and reliable information, and that protects and promotes human rights and democracy.

Everyone, everywhere should be able to participate freely and safely in the creation, consumption, dissemination, and evaluation of information and ideas. The UN's Global Digital Compact calls on states to *work together to promote information integrity, tolerance and respect in the digital space*, and to *promote diverse and resilient information ecosystems.*[1] However, global discourse, initiatives, and policies that address information integrity have been largely focused on the challenges arising from the rapid spread of digital information manipulation, which erodes integrity in the information ecosystem. These concerns more recently include the acceleration of digital information manipulation through developments in generative artificial intelligence. Focusing primarily on the challenges may lead governments, online platforms, civil society, the press, and other stakeholders to overlook the essential ideas, values, and benefits of a healthy information ecosystem.

A healthy information ecosystem should support and advance human rights, in particular freedom of expression, which includes the right to seek, receive, and impart information and ideas of all kinds. This Blueprint emphasizes that we collectively should strive to build, promote and support the creation of accurate, reliable and trustworthy information, rather than only remove, restrict harmful or manipulated content. Governments, the private sector, civil society, academia, and the technical community should work together to promote a shared, positive vision for online spaces. As such, the Blueprint seeks to strengthen multistakeholder approaches to promote information integrity and build civic resilience against digital information manipulation.

The FOC believes a healthy online information ecosystem is fundamental for democracies, which are dependent on open, free, and inclusive public debate and on an environment where people can access a variety of ideas.[2] Furthermore, an information ecosystem that encourages diverse, reliable, trustworthy, and accurate information is a powerful way to address digital information

[1] Global Digital Compact
[2] FOC Joint Statement on Information Integrity Online and Elections

manipulation. This Blueprint is intended to help disentangle complexities and confusion about the online information ecosystem and reinforce a responsible and rights-respecting approach to technology. It suggests actions and identifies opportunities that contribute to the overall aspirational vision of a healthier information ecosystem.

Chapter I - Agency

A human rights-based and a human-centric approach to digital technologies means individuals must be front and center. Individuals and communities should be able to participate freely and safely in the creation and dissemination of information and ideas. They should be empowered to meaningfully, safely, and autonomously be the architects of their own online experiences. We encourage investments by governments, the private sector and other relevant actors along information stack, in efforts that strengthen individuals' civic resilience to digital information manipulation and their ability to engage in the digital realm, including the ability of individuals and communities to generate or produce new outputs, platforms, and applications.

The agency of individuals to participate online is enabled by the tools and opportunities necessary to exercise the right to seek, receive, and impart information as well as to navigate online spaces intentionally and meaningfully. Governments should promote individuals' agency and empowerment through investment in initiatives that build civic resilience to digital information manipulation and improve digital, media, and information literacy[3]. For online platforms, design and transparency choices are crucial to give more agency to users, where users can curate their own experiences online. Lack of understanding of how online platforms shape users' digital information feeds, including lack of algorithmic transparency, has made citizens less resilient to digital information manipulation. Governments and the private sector should work together with civil society to enhance user agency and empowerment based on the four clusters listed below:

1. Literacy: Literacy efforts can build civic resilience to the challenges posed by the dissemination of harmful and manipulated information online such as misinformation and disinformation, hate speech, or harassment, including gendered. Enhanced literacy will equip individuals with the skills to better make meaningful decisions about their participation in the online information environment.
    a. Governments should promote and develop initiatives, including regulation when necessary, to improve literacy aimed at enhancing individuals' understanding of their human rights online and strengthening their ability to identify and contend with digital information manipulation.

[3] In this document, the use of "literacy" refers to both digital, media and information literacy as a whole. We recognize the importance of all these different types of literacy efforts to enhance Agency.

b. Online platforms should strengthen engagement with civil society and governments in order to design platforms and products that support user agency, providing users with more choices to tailor their own online experiences to meet their individual needs. This approach will promote information that better fulfils the desires and aspirations of communities and societies online, especially marginalized groups and peoples;
c. Online platforms should invest more resources and collaborate on Trust & Safety tooling to provide features that support civic resilience, including an informed and reflected engagement with information on their platforms.

2. Privacy: Individuals should not have to fear the risks related to the tracking and predicting of online behaviour, and they should not feel pressured to self-censor due to lack of adequate privacy protections. When governments and online platforms champion privacy needs, and ensure real privacy features and safeguards, they enable people, including those belonging to vulnerable or marginalised groups, to engage with the information ecosystem with fewer risks. Meaningful agency presupposes that people can freely choose their level of privacy online vis-à-vis the services that depend on data collection.
    a. Governments should put in place adequate and foundational privacy regulations;
    b. Governments, online platforms, and civil society should work together to develop innovative ways of data collection and management that protects and strengthens privacy and are more user-centric.

3. Safety: When technology-facilitated violence and cyberbullying, including disinformation campaigns, especially targeted at persons belonging to vulnerable or marginalised groups, are not addressed, chilling effects often result in individuals self-censoring or withdrawing from online and other public spaces. The release of AI- models that can generate synthetic photo and video material, especially when used to create and disseminate non-consensual intimate content, further emphasizes the importance of online safety. When people restrict their expression due to lack of online safety, they lose agency to fully engage online.
    a. Governments should put in place adequate regulations to protect citizens against harmful content and interactions online and human rights violations while protecting freedom of expression and other human rights;
    b. Online platforms should devote sufficient resources to responsibly manage harmful content and interactions online, including sufficient human oversight of content moderation for local contexts and language;
    c. Online platforms should invest more resources to improve the ability of AI to counter harmful content and interactions online in a rights-respecting manner;
    d. Online platforms should devote sufficient resources to engage closely with civil society stakeholders, and take into account diverse lived experiences to ensure online safety in its entirety.

4. Transparency: Users of online platforms should be able to determine why they see what they see; it is essential for all to have the tools to identify how the information they are seeking, receiving, and imparting is being managed. Understanding how digital information feeds are shaped will enable citizens to be more resilient to digital information manipulation.
    a. Online platforms should provide users with options that meaningfully inform them about how their information feeds are shaped, including on how and when AI has been partly or fully used to create a piece of content or communication;
    b. Online platforms should work together to develop and uphold industry standards around authentication, provenance, and verification of AI-generated content, such as the Coalition for Content Provenance and Authentication (C2PA) and the Munich Tech Accord, while protecting privacy and ensuring access globally.

Chapter II - Trust

A trustworthy information environment is fundamental for individuals to exercise their right to freedom of expression. The erosion of trust in the information realm has been steadily diminishing due to technical and socio-political factors, including the challenges related to digital information manipulation. This loss of trust can impair a sense of shared reality and bring about a general distrust or confusion due to an overwhelming amount of information.

Trust is essential for people to engage and participate constructively and meaningfully in society and with one another. One of the main trust relationships is the one between the user and the piece of information itself. Other trust relationships include between users themselves, as well as between the content generator and the content consumer, the user and the platform, and between citizens and policymakers. Users should be empowered to navigate and assess the reliability of information online. Online platforms' design choices that prioritize transparency and user agency, and government policies that promote privacy and accountability also facilitate trust. Extending this trust to users in turn makes possible more reliable trust relationships with content providers and with governing bodies operating within the information ecosystem.

1. Transparency and Accountability: Individuals have a right to hold diverse opinions, and should be enabled to better understand how their digital information feeds are shaped. Individually-tailored information, for instance through the employment use of algorithmically-determined news or information feeds, creates personalized online experiences and realities. This can exacerbate social divisions and increase polarization. Transparency is a key pillar of trust, supported by individual self-determination. The

addition of generative AI, including deep/cheap fakes, audio fakes, and more, has magnified this challenge and further undermines trust in the online experience.

a. Governments should encourage online platforms to enhance platform transparency and communication about infrastructures, algorithms, and users' online information experiences;
b. Governments should encourage online platforms to design products in a rights-respecting manner and to conduct regular human rights due diligence and disclose key findings;
c. Online platforms should ensure that users have access to review design choices and receive communication on the effects of these choices.
d. Online platforms should ensure that information about the functioning of algorithms, especially the recommender systems, and their consequences, is transparent to users and that users may select the degree of targeted information they prefer;
e. Online platforms should ensure users can access information about the creation of information, including whether a piece of information was produced by a human or a bot. Bots and AI-generated content should be labelled in clear and easy to understand fashion. Additionally, content produced by AI should include sources that were used for its production (see reliability of sources).
f. Online platforms should provide researchers and governmental authorities seeking to understand how information feeds are shaped access to relevant data in a manner that respects the privacy of users and protects against unconstrained, unreasonable, arbitrary, or disproportionate access to personal data by government entities.

2. Reliability of sources: For individuals to maintain a reflective and critical approach to online knowledge and information consumption, individuals should be empowered to make informed decisions on the reliability of information and make informed opinions (see Agency). In addition to enhanced platform transparency concerning the use of personal data and platform functioning, users should also be empowered to decide on content exposure and make assessments about sources.
    a. Online platforms should enhance discoverability of sources, while protecting privacy, in order for users to be able to trace the content's origin and make informed assessments of its reliability and trustworthiness.
    b. As content and search is increasingly AI-generated or AI-powered, online platforms should especially consider how to integrate sources of information, including in "AI-overviews" to enhance user trust and maintain reflected engagement with information and knowledge.
    c. Governments and civil society should support traditional media, and especially independent media, because of their unique role in the information ecosystem.

Governments and civil society should also work with journalists to support literacy efforts, particularly as it relates to AI's impact on elections.

d. Governments and the private sector should promote and protect the development of digital public goods to advance inclusive access to knowledge that empowers communities in ways that recognize and protect intellectual property rights, including copyright and trade secrets, confidentiality, privacy rights, and national security.

3. Privacy and Safety: People who publish information, especially persons belonging to vulnerable or marginalised groups, have good reason to fear reprisals by powerful entities and individuals. Trustworthy information environments require strong privacy and data protection regimes to hold governments as well as online platforms accountable for how data is collected, accessed, used, and shared. No data is safe from hacking of systems and services, and no organization can ensure that data shared with it will not be made public. Users should have the ability to decide how much of their personal data to share and be made aware of these risks. To be able to trust the information ecosystem and to freely interact online, users and online communities must feel that their online safety is ensured.
    a. Governments should advocate for and enact legislation that protects users' privacy online. This is especially essential to ensure participation of persons belonging to vulnerable or marginalised groups.
    b. Governments and online platforms should work together to ensure adequate, appropriate and necessary protections of users from online harms, especially those most vulnerable to harassment, discrimination, doxxing, or persecution.
    c. Online platforms should ensure that users have the ability to give meaningful consent about how much of their personal data to share with the platform and with other users.

Chapter III - Inclusion

Democracy flourishes when the voices of individuals are heard and individuals can meaningfully participate in society. Democracy depends on the free exchange of ideas, and being exposed to a variety of ideas is also a key element in the definition of information integrity in the Global Declaration on Information Integrity Online. We understand digital inclusion not only as the access to the internet and online spaces, but also as the quality of the online experience itself.[4]

Promoting digital inclusion and diversity in the design, development, and governance of digital technologies is directly linked to protecting and promoting both the exercise of human rights online,

[4] FOC Joint Statement on Digital Inclusion

in particular freedom of expression, and the open, global, interoperable and reliable Internet.

1. Linguistic and cultural diversity: A lack of linguistic diversity excludes people and communities from the benefits and opportunities of the digital world, including online representation and discourse. It also means that various cultures, places, histories, and names are underrepresented in the digital space and will not exist in the data used to train AI systems. In content moderation processes this can cause linguistic and cultural misperceptions of specific contexts that challenge responses to online harms.
    a. Online platforms should ensure that they can respond to the multilingual needs of their users and that their platforms and services support a wider variety of languages.
    b. Governments and the private sector should work together to ensure greater access to the Internet to promote the growth of other languages, including indigenous and minority languages, online, including considering relevant avenues for funding.

2. Universal Meaningful Connectivity: Continued lack of access to the internet for about one third of the world's population means that too many people are still unable to participate meaningfully in society. However, Internet access is about more than infrastructure. Universal and meaningful access should address social and economic barriers, including affordability of devices and access as well as socio-political barriers that prevent individuals, especially women, from participating online.
    a. Governments and the private sector should engage with multistakeholder networks to comprehensively address barriers to achievement of meaningful Internet access;
    b. Governments should commit to expanding infrastructure, including by developing innovative and blended financing mechanisms and incentives, in line with the Sustainable Development Goals;
    c. Governments should engage with and support community networks to successfully bridge the connectivity gap and help communities build the internet infrastructure and skills they need to participate fully in digital society;
    d. Governments should undertake national assessments of meaningful access to the Internet, for example by following UNESCO's ROAM-X indicators.

3. Promotion of diverse and global voices: Communities represent a diversity of voices. Diverse perspectives are at the core of democracies. Diversity of voices and opinions can be an antidote to digital information manipulation by promoting counter-narratives and addressing the increasing polarization online and offline.
    a. Online platforms should invest in research that explores how to optimize for diversity of voices in their platform designs;
    b. Online platforms must consider and address the consequences of further excluding already marginalised voices online, as algorithmic curation and recommender

systems systemically risk lowering the diversity of voices, especially for already underrepresented communities, especially vulnerable and marginalised people;

c. Governments should explore policies to support quality, independent and local media, and journalism, as well as other forms of civic information and knowledge production, such as public memory, public archives, and civic forums.

4. Protection against non-discrimination and harassment: Online harassment and abuse have a severe chilling effect on the ability of people to exercise their freedom of expression or participation in public life. Marginalized groups – including women, LGBTQ+ individuals, and people with disabilities – are disproportionally targeted with online violence.
    a. Online platforms should ensure meaningful stakeholder engagement to fully address the various harms, including harassment, violence and discrimination, stemming from their services and platforms, and to inform platform policies and design;
    b. Online platforms should continuously conduct human rights impact assessments and include diverse voices and lived experiences;
    c. Online platforms should invest necessary resources in developing trust and safety tooling to effectively address harassment, discrimination and violence on their services and platforms, including as consequences of algorithmic curation, and of bias in and from AI models, including generative AI.;
    d. Governments should consider necessary and appropriate regulation, developed through multistakeholder consultations, that holds online platforms accountable for potential human rights abuses on their platforms and services;
    e. Governments should ensure comprehensive literacy programs, starting at school level, to support young people and kids to navigate a digital life.

Resources

- FOC Joint Statement on Digital Inclusion
- FOC Joint Statement on Information Integrity Online and Elections
- Global Declaration on Information Integrity Online
- The Action Coalition on Meaningful Transparency - Global Repository
- Santa Clara Principles
- Integrity Institute - Shining a Light on Platform Transparency Best Practices
- The 2022 Code of Practice on Disinformation
- InternetLab's work on Privacy and Surveillance
- Observatory of Political Violence
- Masakhane
- Alliance for Affordable Internet (a4ai.org)
- IGF's Policy Network on Meaningful Access (PNMA)
- Internet Universality Indicators | UNESCO
- Connect Humanity
- ECNL - Framework for Meaningful Engagement
- Freedom Monitor Observatory

- International Observatory on Information & Democracy
- Digital Trust & Safety Partnership
- United Nations Global Principles for Information Integrity
- OECD Hub on Information Integrity
- Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse
- Democratic Roadmap: Building Civic Resilience to the Global Digital Information Manipulation Challenge