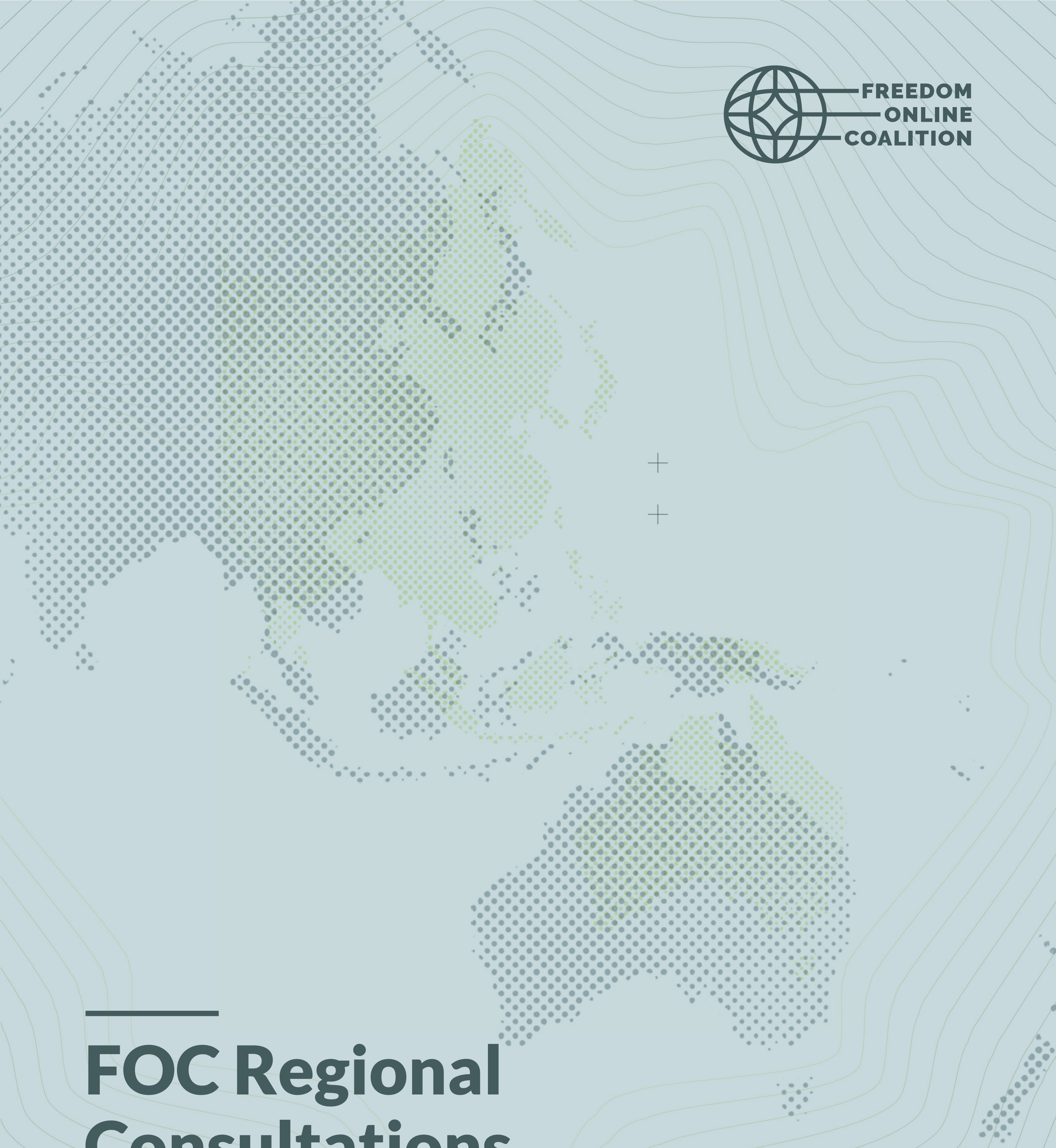
FREEDOM
ONLINE
COALITION



FOC Regional Consultations

Summary of Regional Consultation
in Asia-Pacific

June 2022

Table of Contents

Context

- As 2022 Chair of the Freedom Online Coalition (FOC), Canada facilitated six multi-stakeholder regional consultations to engage directly with stakeholders and gather knowledge about Internet freedom challenges at the regional and sub-regional level.

- The multi-stakeholder consultations will feed into the FOC's upcoming "Ottawa Agenda", which will update the Coalition's founding document, the **Tallinn Agenda**, with a set of commitments for promoting human rights online.

Summary

- During the Asia-Pacific regional consultation held under Chatham House Rule, experts from civil society, media, academia, and the private sector highlighted that the FOC can continue to play a convening role for diverse stakeholders and proposed a number of policy, programming and engagement approaches for members to support digital inclusion and target the misuse of digital technologies.

- Digital exclusion has negative consequences for individuals, communities and national development. With the Internet increasingly seen as the voice of the people, those not online are in danger of being marginalised.

- Digital safety and civic participation remain core concerns. Social media is rife with disinformation and threats to users. Some public and private actors 'weaponize' disinformation, while tech platforms may lack proper incentives or regulation to tackle harmful practices.

- In promoting digital inclusion, more needs to be done to engage youth and women on issues such as cyber-bullying, online gender-based violence, and identifying reliable news sources.

Trends

Experts agreed that digital inclusion is now vital for individuals, communities, and national development. In a world in which access to services is increasingly digitalized, connectivity and digital literacy are imperative to reduce poverty and deliver a range of public and private goods. At the same time, much of the current agenda around digitalization and artificial intelligence is closely bound up with issues of data ownership and control, reinforcing divisions between the haves and have-nots.

Connectivity and **literacy** were widely recognized as two large and challenging pieces of the international structure that is being assembled around digital technologies. The first relies heavily on governments and large private sector actors to put key infrastructure in place, while the second speaks primarily to the need to enhance the capabilities of much of the world's population to constructively and safely use digital tools.

Meaningful connectivity ensures the availability of infrastructure, devices and affordability. Policy has become *"tuned to connected people"*, with one participant asking: "Are we making policy which is optimized for both digital and non-digital infrastructure?" Product development is limited by the language capabilities of programmers using open source software, making it difficult to develop localized security patches and increasing the vulnerability of end users.

From the standpoint of gender equality, it was suggested that more emphasis be placed on women and coding, for the FOC to incorporate feminist principles for the Internet, and that there be a digital component to the women, peace and security agenda. Others emphasized the importance of youth engagement on **digital literacy** – sensitizing youth to the issues they will need to address, including cyber-bullying and online gender-based violence. It was recommended that the FOC deepen its engagement with academia on these and other issues, ensuring, for example, that leading research on policy helps to *"bridge the disconnect"* between youth and mainstream media. One expert noted that citizens who are excluded from media are often consuming *"fringe media"*.

Participants felt transparency and accountability are lacking in many areas of digital governance and technology, with legal frameworks *"built on control and surveillance"*. The possibility for technology to fuel discriminatory practices – for example, through electronic identification based on religion, ethnicity or locality – was underlined by a number of participants.

A prominent thread in the discussion was that technology providers and online platforms often seem unwilling or unable to self-regulate adequately. It was also noted that there is a financial disincentive for platforms to address problematic content if it drives engagement and creates profitable metadata. When fact checking becomes a financial liability – and if no further requirements are imposed – it can support the *"monetization of disinformation"*.

Experts noted that in many geographic contexts, social media is largely *"becoming the Internet"* and that the experience of some countries' political campaigns in using **disinformation** is being exported. Disinformation was also noted as a serious threat during the pandemic, spurring negative health outcomes. There was broad agreement that the base Internet is still important and that *"those who are not on social media are still relevant,"* though on many issues – ranging from climate change to urban poverty – civil society saw social media as the principal tool to help organize activism and give voice to underrepresented narratives. Media representatives worried that purveyors of disinformation are hijacking social media platforms and predicted more widespread use of deep fake technology.

One expert suggested that the FOC develop a framework for countering disinformation campaigns, including *"pre-bunking,"* (i.e., highlighting misleading or manipulative strategies and outlining ways to neutralize the disruptive potential of disinformation before people encounter it).

The Internet is increasingly viewed as the main vehicle for free expression, so those not online are *"in danger of being ignored"*. **Internet shutdowns** have major effects in remote areas such as archipelagos and for the rural poor. Social media is a major source of threats and abuse targeting human rights defenders, with accounts increasingly being *"weaponized"*, while the number of online *"safe zones"* decreases as governments target VPN service providers. Knowledge around safe use of the Internet and **cyber security** remains low in many countries in the region, while access to security software is limited by both availability and affordability.

One private sector participant urged that, in some cases, FOC countries consider the use of extraterritorial legislation to adopt and extend standards beyond national boundaries. Also at the governance level, participants highlighted the importance of sufficient protection against cyber-bullying and suggested that **cyber security** measures *"should be built into the system"*.

Several participants suggested that some governments may seek to use **Internet fragmentation** to their advantage, for example in political campaigning. Independent media is needed to *"set the tone"* in factual conversations about the opportunities/benefits of open Internet and the risks/societal implications of fragmentation, while governments should be *"protectors"* of citizens and public goods – preventing a range of harms and not just hate speech, "or else the same actors will continue to dominate."

Participants expressed concern that illegal **spyware** is helping to create a powerful surveillance ecosystem with little protection for ordinary people. It was suggested that FOC members consider different mechanisms, such as the use of export controls, regulations or sanctions on the sale, transfer or use of such technologies. It was also recommended that FOC members be more active at the International Telecommunication Union to help update its cyber security policies.

More broadly, the FOC was urged to assist civil society to integrate digital technologies and safe practices and to inform newly connected communities on how to self-educate. Participants also expressed concern that the financial challenges faced by many media outlets can encourage a proliferation of clickbait and disinformation, which may further erode public trust in online media. Experts recommended that some FOC members should be more active in the region.

It was agreed that the UN Guiding Principles (UNGPs) provide an important framework for sharing best practices and that *"applied knowledge creates impact."* An *"imposition approach"* is unlikely to be productive, but there is a convening role for the FOC to play in spreading awareness of key principles, in helping to *“enable better platforms”*, and in working with private digital and internet service providers to encourage adherence to international standards/principles – particularly as *“all these major organisations are eager to meet the Sustainable Development Goals”*. Engagement with the grassroots is also crucial: in the right enabling environment, stakeholders can disseminate information to the public directly and effectively.

Recommendations

Participants recognized that the FOC remains relevant and can and should do more, taking timely and decisive action to address the misuse of digital technologies, but also contributing to the larger challenges associated with global governance, connectivity and digital literacy through research and advocacy. Participants recommended several actions that FOC members, individually or collectively, could undertake to increase Internet freedom regionally and worldwide. The FOC should:

- Continue to promote the benefits of digital inclusion to partners in the Global South, including non-FOC States.

- Take more assertive action on issues such as nefarious use of surveillance technologies, disinformation campaigns, and Internet shutdowns, including the development of regional or country-based consultative focal points or meetings of FOC member embassies to provide stronger regional-level knowledge and reporting to the FOC and country headquarters on laws, policies and practices.

- Consider the use of export controls, regulations or sanctions on the sale, transfer or use of surveillance technologies.

- Be more active at the International Telecommunication Union to help update its cyber security policies.

- Develop a framework for countering disinformation campaigns, including “pre-bunking,” i.e. highlighting misleading or manipulative strategies and outlining ways to neutralise the disruptive potential of disinformation before people encounter it.

- Assist civil society to integrate digital technologies and safe practices and to inform newly connected communities on how to self-educate.

- Pay closer attention to, and monitor through research and reporting, national and regional trends, including human rights due diligence exercises by the private sector within their realm/countries.

- Convene local multistakeholder networks to address issues and build trust to work together proactively; engage in more public awareness and advocacy programs; and contribute to capacity building efforts for media advocacy and training.

- Expand its multi-stakeholder engagement to include youth voices.

- Continue discussions with the private sector on the main transnational issues surrounding digital technology – including transparency, accountability and governance – recognizing that online users are at once citizens (for governments) and consumers (for the private sector), and that there must be shared approaches to some of the most challenging issues at hand (e.g., disinformation).

Annex

Discussion Questions

- What regional or global trends related to the evolution of digital technologies and the internet will have the greatest impact on human rights online and offline in the coming 5-10 years?

- What are the most pressing challenges to the protection and promotion of human rights online, both regionally and internationally?

- How do we define free, open, interoperable, secure and reliable Internet at the infrastructure and governance levels? How can governments defend against Internet fragmentation?

- Where should governments focus their attention and international assistance support in bridging digital divides and increasing digital literacy?

- How should the FOC respond to growing attempts made to restrict democratic voices online (i.e. internet shutdowns, disinformation, spyware technologies)?

- What programs, initiatives or processes should the FOC engage on in the next 5-10 years to help protect human rights and fundamental freedoms and advance meaningful digital inclusion?

- How can the FOC deepen dialogue and cooperation with the private sector on the effective implementation of the UN Guiding Principles on Business and Human Rights?