

CIVIL SOCIETY ADVOCACY TOOLKIT

Engaging Technology Companies on Human Rights in Asia-Pacific

For civil society organisations working on freedom of expression, privacy, and digital rights in the Asia-Pacific region.

HOW TO USE THIS TOOLKIT

This toolkit is structured to move you from understanding to action. You can read it cover to cover, or jump directly to the section most relevant to your current work:

- Need a human rights grounding? → Human Rights Framework (p. 3)
- Planning to engage a tech company? → Safe & Strategic Engagement (p. 5)
- Operating in a high-risk context? → CLARITI Shadow Assessment (p. 7)
- Seeking international levers? → Advocacy & Accountability (p. 9)

Introduction

Technology companies now sit at the heart of public life across Asia-Pacific. Social media platforms, telecommunications providers, cloud infrastructure operators, and artificial intelligence developers shape how people communicate, access information, and participate in civic space.

Governments throughout the region are moving fast to regulate the digital environment — through cybersecurity laws, online content controls, data localisation requirements, and platform governance frameworks. Some of these measures address genuine public interests. Others risk enabling censorship, mass surveillance, and the systematic suppression of civil society.

In this context, civil society organisations (CSOs) are indispensable: documenting harms, amplifying the voices of affected communities, and holding both states and corporations to account against international human rights standards.

What this toolkit helps you do

- **Assess** technology-related human rights risks in your operating context
- **Document** harms experienced by communities in a credible, structured way
- **Engage** technology companies responsibly and safely
- **Advocate** for stronger accountability — locally, regionally, and internationally

Human Rights Framework for Technology Companies

International human rights law provides the primary foundation for holding technology companies to account. The frameworks below are the most frequently cited in digital rights advocacy — knowing them equips you to engage companies and policymakers with credibility and precision.

Core International Standards

Standard	Relevance to Tech Companies
Article 19, UDHR & ICCPR	Protects freedom of expression , including the right to seek, receive and share information online across any media or platform.
Article 17, ICCPR	Protects the right to privacy , guarding individuals against arbitrary interference with their communications and personal data.
UN Guiding Principles on Business & Human Rights (UNGPs)	Establishes that companies — not only states — must respect human rights, avoid harm , and conduct ongoing human rights due diligence.

The UNGPs are especially critical for tech advocacy: they establish that companies must respect human rights independently of whether governments require it, and that they must address adverse impacts linked to their operations — including impacts on content governance, data management, and platform design.

Regional Frameworks: ASEAN

When engaging companies operating in Southeast Asia, the following ASEAN frameworks provide relevant regional context. While primarily focused on economic development and digital connectivity, they create openings for civil society to embed human rights considerations:

- [ASEAN Digital Masterplan 2025](#)
- [ASEAN Framework on Digital Data Governance](#)
- [ASEAN Digital Economy Framework Agreement \(DEFA\)](#)
- [ASEAN ICT cooperation mechanisms](#)

Sector-Specific International Instruments

- [UN B-Tech Project](#) — practical guidance on applying the UNGPs specifically to digital technologies
- [Global Network Initiative \(GNI\) Principles](#) — widely referenced standards for ICT companies on protecting freedom of expression and privacy
- [Santa Clara Principles](#) — transparency and accountability benchmarks for content moderation
-

WHY THIS MATTERS FOR YOUR ADVOCACY

Many technology companies cite these frameworks in their transparency reports and public policies. Knowing them allows you to hold companies to their own stated commitments — not just abstract principles.

Engaging Technology Companies Safely and Strategically

In high-risk and conflict-affected countries, engaging technology and ICT companies requires careful preparation. The guiding principle throughout must be do no harm — to your organisation, your partners, and the communities whose experiences you represent.

The [CSO Guidelines for Engagement with ICT Companies in Conflict-Affected and High-Risk Areas](#) (George Washington Law Clinic) outlines what meaningful preparation looks like: analysing the conflict context, clarifying your objectives and principles, assessing security and data-protection risks, and developing clear messages before any engagement begins.

The practical recommendations below complement those guidelines.

Six Principles for Responsible Engagement

01 Do Your Homework	Research the company's policies, enforcement history, and legal obligations before making contact. For example, Meta's transparency reports document how the company restricts content in response to government requests — this gives you a baseline for what you're challenging.
02 Engage the Right People	Target teams responsible for human rights, policy, trust and safety, or legal compliance — not just public-affairs staff. Relevant contacts can often be identified through company policy pages, LinkedIn, public consultations, and regional office directories.
03 Act Collectively	Coordinate with peer CSOs and allies to avoid fragmentation and build collective leverage. Check whether regional coalitions are already active — such as the South East Asia Collaborative Policy Network (SEA CPN) or the ASEAN Regional Coalition to Stop Digital Dictatorship.
04 Prioritise Safety	Assess risks before and after engagement. Use secure communications. Consider what reprisals are possible and plan mitigation measures in advance.
05 Document Everything	Keep detailed records of all concerns raised, commitments received, and agreed follow-up actions. Documentation is both your accountability tool and your evidence base.
06 Escalate When Needed	If direct engagement fails, escalate. Use collective advocacy, regional accountability mechanisms, and community-led tools such as CLARITI (see next section) to build external pressure.

CLARITI: Community-Led Shadow Human Rights Impact Assessment

In contexts where direct engagement with technology companies is unsafe or impossible, civil society organisations can still build a compelling, evidence-based advocacy position — by conducting their own human rights impact assessments.

[CLARITI](#) is a practical, community-led tool that enables civil society to convert lived experience into credible human rights evidence. Developed by ARTICLE 19 and Ranking Digital Rights, it allows CSOs to carry out ‘shadow’ human rights impact assessments (HRIAs) when companies do not publish their own assessments, conduct them behind closed doors, or fail to consult affected communities meaningfully.

CLARITI follows an eight-phase process designed to give civil society a rigorous, defensible structure for their research:

Phase	What Happens
1. Define purpose	Clarify the scope, objectives and audience for the assessment
2. Prepare the team	Build the research team and identify affected stakeholders
3. Scope issues	Map the key human rights concerns to investigate
4. Analyse legal context	Examine the applicable legal and policy environment
5. Document impacts	Gather evidence of harm experienced by affected communities
6. Develop recommendations	Formulate concrete asks for companies and governments
7. Compile findings	Structure findings into a credible, publishable report
8. Use the results	Deploy findings in company engagement and wider advocacy

CLARITI has already been deployed in high-risk contexts across the region, producing evidence that was previously invisible to international audiences:

Case Study: Vietnam

[Legal Initiatives for Vietnam](#) applied CLARITI to assess Facebook’s operations in the country. *The assessment documented how activists, independent media, and civil society organisations experienced wrongful content removals, account restrictions, reduced visibility, and the amplification of state propaganda* — harms that had not previously been formally evidenced at the international level.

Case Study: China

[Human Rights in China](#) used CLARITI to assess X (formerly Twitter) as a critical platform for Chinese human rights defenders and dissidents. The assessment identified *arbitrary account suspensions, shadow banning, over-reliance on automated moderation, and abuse of the platform’s verification system* — which enabled impersonation, harassment, and phishing attacks against activists.

⚠ SAFETY FIRST

CLARITI is designed for use in contexts where direct engagement with companies may not be safe. If your operating context involves significant risks, consult your organisation's security protocol before beginning any assessment process.

Using Findings for Advocacy and Accountability

Once you have documented evidence — whether through CLARITI or other methods — you have multiple pathways to amplify it. The most effective strategies combine local evidence with international accountability mechanisms to create pressure from multiple directions simultaneously.

Strategic Recommendations for International Advocacy

The following recommendations are designed for regional CSOs beginning to engage with business and human rights (BHR) issues in the technology sector.

1 Use CLARITI findings in UN processes

Bring documented evidence to the [UN Asia-Pacific Forum on Business and Human Rights \(UNRBHR\)](#) and engage the [UN B-Tech Project](#) for additional policy support.

Propose targeted session formats — for example, a 'community-led HRIA clinic' or a 'company accountability roundtable' — and use these convenings to secure follow-up meetings with companies and governments who attend. Other relevant UN mechanisms include the UN Special Rapporteur on Freedom of Opinion and Expression, the Special Rapporteur on the Right to Privacy, and the Universal Periodic Review (UPR).

2 Push for operational commitments through industry channels

Engage business-focused forums to move discussions beyond general principles toward concrete commitments: greater transparency in handling government requests, clear escalation channels for CSOs, and meaningful community consultation within human rights due diligence processes.

Do not limit yourself to international platforms. Chambers of commerce, industry associations, and consumer unions can also be effective entry points for raising these issues directly with companies.

3 Work within cross-constituency networks

Bring CLARITI outputs into networks such as the [Global Network Initiative \(GNI\)](#) that bring together technology companies, institutional investors, and human rights experts. Engaging companies and investors in the same space creates compounding pressure and improves the likelihood of meaningful follow-up.

4 Amplify evidence through accountability platforms

Coordinate with the [Business & Human Rights Resource Centre \(BHRRC\)](#) or the B-Tech Project to raise the visibility of documented harms and create a formal company response trail — particularly useful when direct engagement has stalled or been refused.

5 Complement forum advocacy with harder accountability routes

If a company is headquartered in — or covered by — an OECD-adhering state, an [OECD National Contact Point \(NCP\)](#) complaint can be a powerful complementary lever, especially when voluntary dialogue has failed.

6 Build a coalition evidence package ahead of major fora

The ASEAN Regional Coalition to Stop Digital Dictatorship and the [Southeast Asia Collaborative Policy Network \(SEA CPN\)](#) have achieved significant advocacy wins through coordinated, pre-event evidence packages.

Before any major intervention, coordinate a brief package covering: (a) two or three concrete findings, (b) a summary of risks and impacts, and (c) five clear asks for companies and governments. This enables international partners to align quickly and speak with a unified voice.

Multi-Stakeholder Platforms Worth Engaging

- [UN Forum on Business and Human Rights](#) — Geneva and Bangkok sessions; key for norm-setting and company accountability
- [Digital Rights Asia-Pacific Assembly \(DRAPAC\)](#) — regional CSO convening with direct industry participation
- Tech-sector summits and industry convenings where companies engage on digital rights issues
- Regional multi-stakeholder processes under ASEAN and UN frameworks

Conclusion

Across Asia-Pacific, digital environments are becoming more constrained. The responsibility to uphold freedom of expression and privacy cannot rest with governments or technology companies alone — it requires sustained, informed engagement from civil society.

Experience from across the region demonstrates that when CSOs document harms rigorously, ground their advocacy in international human rights law, and act collectively, they can meaningfully influence even the most powerful technology actors — including those operating under restrictive state conditions.

The lesson for human rights practitioners is clear: strategic, evidence-driven engagement is not merely possible in high-risk contexts — it is essential. Digital technologies will continue to reshape civic space across Asia-Pacific. Whether those technologies develop in ways that respect dignity, protect rights, and strengthen democratic participation depends, in no small part, on whether civil society chooses to engage.

GET STARTED

Ready to use this toolkit? Here are your immediate next steps:

- Review the human rights frameworks most relevant to your target company or government
- Map your operating context against the safety checklist in the Safe Engagement section
- Explore CLARITI at claritihria.net if a shadow assessment is appropriate for your context
- Connect with SEA CPN or DRAPAC to identify existing coalitions you can join