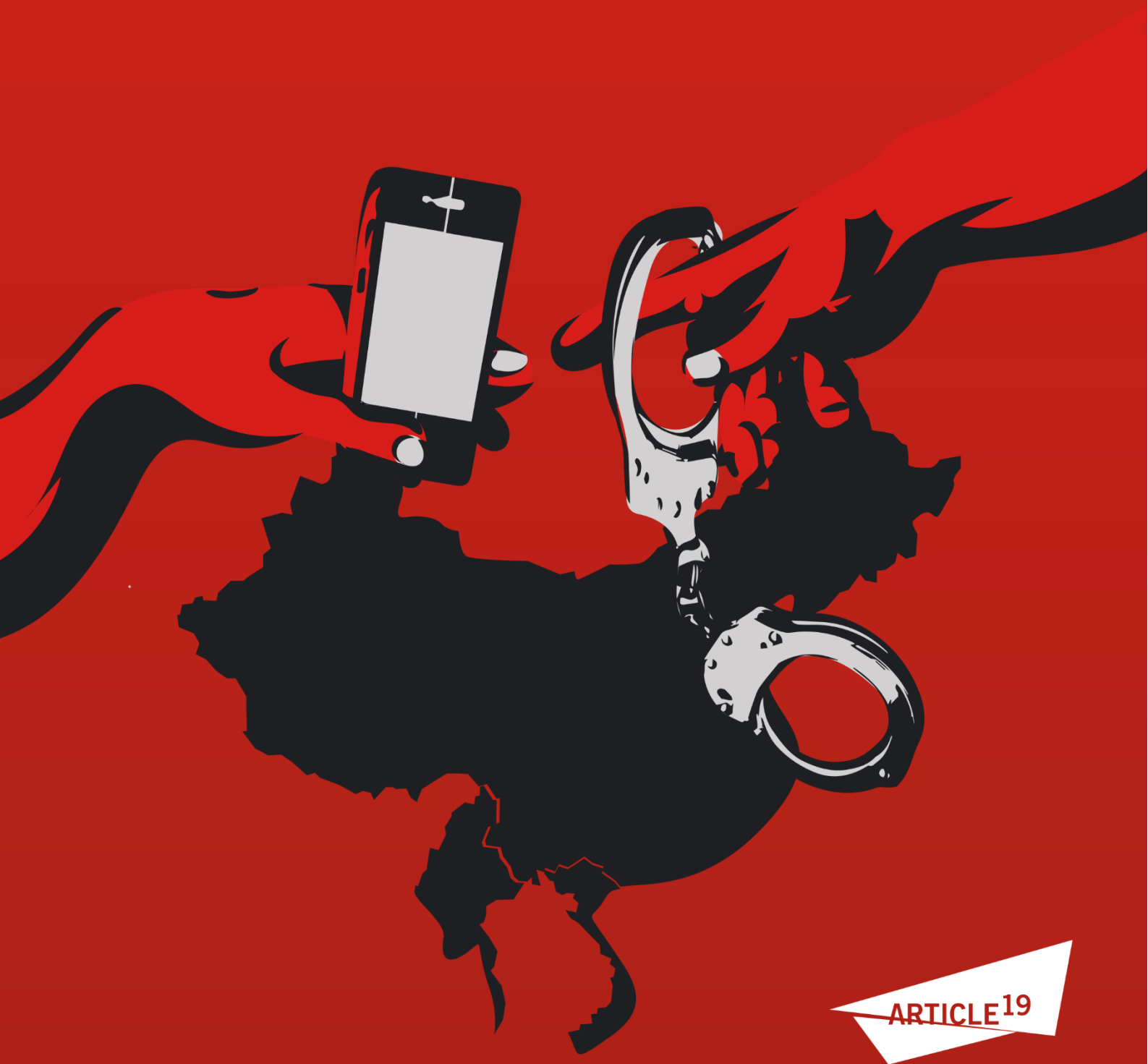
Human rights responsibilities and challenges for tech companies operating in authoritarian countries



ARTICLE 19

ARTICLE 19

72–82 Rosebery Ave
London EC1R 4RW
UK
www.article19.org

T: +44 20 7324 2500
F: +44 20 7490 0566

E: info@article19.org
W: www.article19.org

Tw: @article19org
Fb: facebook.com/article19org

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices.

Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our 9 regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on 5 key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used. The report was developed as a part of the **Engaging Tech for Internet Freedom (ETIF)** initiative, under funding from the US Bureau of Democracy, Human Rights, and Labor. The Centre for Law and Democracy played a valuable role in preparing this report. ARTICLE 19 bears the sole responsibility for the content of the document.

Executive summary

In this report, ARTICLE 19 reviews the human rights context and responsibilities of tech companies operating in 3 authoritarian countries in Asia, namely China, Myanmar, and Vietnam. It focuses on the rights to freedom of expression and privacy, and the manner in which authoritarian states directly or indirectly expect companies to assist them in censoring content, promoting propaganda, accessing user data, and engaging in surveillance. While these are undoubtedly highly challenging contexts, companies have not sufficiently prioritised protecting human rights in their policies and actions.

States are the primary duty bearers under international human rights law, but companies also have human rights responsibilities, as outlined in the United Nations Guiding Principles on Business and Human Rights (UNGPs). Even if domestic law or circumstances make it impossible for companies to fully meet their human rights responsibilities, they should take action so as to respect human rights standards to the greatest extent possible. Tech companies should not merely reference local law as an excuse for collaborating in rights violations. They should take steps such as those detailed in this report, like adopting appropriate policies, asking governments to justify content removal requests clearly and specifically, and reporting transparently on their compliance with government demands.

For each country, we survey the country context and provide an overview of legal obligations which companies operate under that are problematic from the perspective of international human rights law and that may, as a result, put pressure on companies to become complicit in violations of the rights to freedom of expression and privacy. We then explore how Western tech companies operating in these countries, many of which have explicitly stated their commitment to respecting freedom of expression and privacy, have responded to these legal obligations and to other government expectations that they will cooperate in violations of these rights.

In China, companies are expected to cooperate broadly in state censorship and surveillance, and to comply with other human-rights-abusive demands. Partly due to the problematic lack of transparency around internal decision-making, there is no way of knowing how these companies view the relationship between their corporate human rights responsibilities and local laws and policies that conflict with international human rights law.

The situation is more mixed in Vietnam, where companies have experienced pressure but also have more space to challenge government demands. However, many companies seem to prioritise business interests and do not act consistently to protect human rights.

In contrast, in Myanmar, after a brutal military regime took control in a 2021 coup, some companies refused to cooperate with the military, recognising it as an illegitimate government, and adopted Myanmar-specific policies. Follow-through on these policies has

been inadequate, however, and companies have lacked the rigorous response needed for this dangerous and complex context.

Tech companies operating in authoritarian contexts often face real challenges in navigating a legal and political landscape that is hostile to freedom of expression and privacy. However, too often they merely cite domestic law as justification for collaborating in rights violations, without making sufficient effort to mitigate human rights harms or limit cooperation to the minimum necessary. It does not appear to be common for them to employ rigorous human rights due diligence or to incorporate human rights standards into decision-making processes. Far greater industry efforts are needed to ensure that companies act in accordance with the UNGPs when operating in authoritarian countries.

Summary of recommendations

ARTICLE 19 calls on **governments in the region** to:

- revise their legal frameworks to bring them into line with international human rights standards, including on freedom of expression and privacy;
- recognise their responsibilities under the first pillar of the UN Guiding Principles (UNGPs) and human rights law, and avoid compelling or pressuring companies to breach their human rights responsibilities;
- foster universal access to an open internet, avoiding shutdowns and unnecessary restrictions on online platforms and facilitating a vibrant online ecosystem; and
- protect human rights defenders and activists, including by taking measures to prevent harassment, threats, or violence against them; immediately and unconditionally release individuals who have been wrongly detained or imprisoned solely for exercising their right to freedom of expression and other human rights.

We call on **tech companies operating in authoritarian contexts** to:

- uphold human rights standards in accordance with the UNGPs;
- conduct human rights due diligence, including by undertaking regular human rights impact assessments; these should be country specific and disclosed publicly, the process should be transparent and should involve meaningful consultation with affected stakeholders, and once assessments are completed, effective measures should be put in place to mitigate identified risks;
- develop, publish, and fairly apply clear policies and procedures for content moderation, including specific standards for responding to government requests to remove content, and ensure that they reflect the principles articulated in the Santa Clara Principles;
- develop clear policies on how they will respond to government requests to restrict services or share user data that include reasonable efforts to resist such requests, such

as a commitment to evaluate each request individually and challenge the legality of requests as appropriate;

- prioritise transparency and accountability: transparency reports should be more regular (ideally monthly) and more detailed than is currently standard practice and should include country-specific commentary on steps taken to comply with and challenge local law, as well as more details on content which has been removed at the request of both governments and users; companies should also be transparent about how they negotiate the conditions for market access, as well as any licences, contracts, or permissions they receive from the government;
- provide tools for user privacy and security: implement privacy by design and empower users to control their personal data;
- ensure appropriate support for their local country teams, including rapid responses and assistance when human rights concerns are raised by local or regional staff;
- support freedom of expression initiatives in the Asia region, such as through providing financial support and technical expertise and collaborating with civil society and other human rights defenders; and
- engage in multi-stakeholder and industry-wide dialogue and pursue initiatives designed to enhance industry-wide collaboration on human rights issues.

Contents

Introduction

Across the Asia region, an explosion in internet use in recent decades has coincided with a rise in authoritarianism in several countries. Governments in these countries are increasingly pursuing repressive tactics and using more sophisticated technical surveillance tools against those who express themselves online.

Many global tech companies have enthusiastically pursued users in Asian markets, often without careful assessment of the human rights challenges involved when operating under authoritarian regimes. These companies must now decide how to respond to regulatory contexts which suppress freedom of expression and privacy. In some countries, tech companies face legal and policy demands to cooperate directly in human rights abuses.

In this report, ARTICLE 19 examines such challenges in 3 countries governed by particularly authoritarian regimes – China, Vietnam, and Myanmar – in order to identify strategies for advancing business respect for human rights even where the domestic situation is not favourable to this. For each country, we provide an overview of the current context and the legal environment for tech companies operating there. We then look at how tech companies have responded to government demands, providing case studies which highlight where companies have been complicit in human rights abuses and where they have tried to push back. Based on international human rights standards on freedom of expression and privacy, as well as the United Nations Guiding Principles on Business and Human Rights (UNGPs), we make practical recommendations for improving tech companies' respect for human rights in authoritarian contexts.

Although we provide recommendations to governments and companies operating in authoritarian contexts, we believe that the support and collaboration of international, regional, and local civil society is crucial to address the practices we document. International groups and coalitions need to work together and with funders to find ways to support local civil society groups working on issues of freedom of expression and privacy, taking into consideration the realities of conducting advocacy in authoritarian contexts. In particular, we believe it is necessary to build networks and connections between civil society organisations based in authoritarian countries and those based in countries where tech companies are headquartered, to amplify the voices of those impacted by rights violations. Civil society should also continue to engage in public campaigns to challenge tech companies when they fail to uphold their human rights responsibilities, as this has often been the most effective avenue for triggering company action. Last but not least, civil society organisations should expand advocacy focusing on the economic and business harms of human-rights-abusive laws and policies, including in partnership with industry groups and tech companies, to supplement human rights-based advocacy. They should also continue to undertake research to expose abuses, develop best practices, and prepare tools and resources to help tech companies better understand and implement the UNGPs in authoritarian contexts.

International human rights standards

Freedom of expression and privacy under international human rights law

The **right to freedom of expression** is guaranteed in Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). It encompasses a right not only to express oneself but also to seek and receive information and ideas. This includes the right to express oneself online and to access information online.

The **right to privacy** is protected in Article 12 of the UDHR and Article 17 of the ICCPR. The latter provides: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'.

States can restrict these rights only in limited circumstances. Freedom of expression may be restricted only according to a three-part test outlined in Article 19(3) of the ICCPR, namely where restrictions: (i) are provided for by law and formulated with sufficient precision to enable those covered by them to understand what is prohibited; (ii) pursue one of the legitimate aims explicitly enumerated in Article 19, such as national security, public order, or the rights or reputations of others; and (iii) are necessary (and proportionate) to protect that legitimate aim.[1] Similarly, an interference with the right to privacy is legitimate only if it is prescribed by law, aims to protect a legitimate aim, and is necessary to achieve such protection.[2]

Both of these rights should be protected online as well as offline.[3] This means that restrictions on the rights in the online context should also be prescribed by law, aim to protect a legitimate aim, and be necessary to protect that aim. For freedom of expression, for example, official requirements to filter internet content are not sufficiently tailored and precise to pass the three-part test for restrictions. State-imposed filtering systems are a form of prior censorship that is not acceptable under human rights law.[4] Blocking websites is also a means of silencing an author or publication, which can only be justified if it targets clearly illegal content that can be restricted under human rights law, such as explicit sexual images of children. Broader measures, such as blocking a widely used social media site, are disproportionate and have indiscriminate impacts, and so cannot be justified under the three-part test.[5]

---

[1] Human Rights Committee, General Comment No. 34, 2011.

[2] Office of the High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age, A/HRC/39/29, 3 August 2018, para 10.

[3] UN Human Rights Council (UNHRC), Resolution 20/8, 16 July 2012.

[4] Organization for Security and Co-operation in Europe (OSCE), Joint Declaration on Freedom of Expression and the Internet, 2011, para 3.

[5] OHCHR, Report on Internet Shutdowns, 13 May 2022, para 13.

Freedom of expression and intermediary liability

At the international level, several human rights bodies and mechanisms have developed soft law guidance on freedom of expression online and intermediary liability, generally maintaining that intermediary immunity from liability is critical to protecting freedom of expression online.

The UN Human Rights Council (UNHCR) affirmed in 2018 that the 'same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice'.[6] The UN Human Rights Committee has made clear that limitations on electronic forms of communication or expression disseminated over the internet must be justified according to the same criteria as non-electronic or 'offline' communications, as set out above, while taking into account the differences between these media.[7]

While international human rights law places obligations on states to protect, promote, and respect human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights and to address adverse rights impacts of their business operations.[8] In meeting their obligations, states may have to regulate the behaviour of private actors in order to ensure the effective exercise of the right of freedom of expression.

Importantly, the UN Special Rapporteur on freedom of expression has long held that censorship measures should never be delegated to private entities.[9] In their 2011 Joint Declaration on Freedom of Expression and the Internet, the 4 freedom of expression mandate holders stated that, at a minimum, 'intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression'.[10]

In his June 2016 report to the UNHRC,[11] the UN Special Rapporteur on freedom of expression enjoined states not to require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means. He further recognised that 'private

---

[6] UNHRC, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/38/L.10/Rev.1, July 2018.

[7] Human Rights Committee, General Comment No. 34, paras 12, 39, 43.

[8] The United Nations Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The UNHRC endorsed the guiding principles in Resolution 17/4, 16 June 2011.

[9] UNHRC, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, A/HRC/17/27, 16 May 2011, paras 75–76.

[10] OSCE, Joint Declaration on Freedom of Expression and the Internet, 2011.

[11] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 May 2016, paras 40–44.

intermediaries are typically ill-equipped to make determinations of content illegality',[12] and reiterated criticism of notice and takedown frameworks for 'incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation', i.e. the danger of 'self- or over-removal'.[13]

The UN Special Rapporteur on freedom of expression recommended that any demands, requests, and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and must demonstrate a necessary and proportionate means of achieving one or more aims under Article 19(3) of the ICCPR.[14]

In their 2017 Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda, the 4 international freedom of expression mandate holders further expressed concerns at 'attempts by some governments to suppress dissent and to control public communications through … efforts to "privatise" control measures by pressuring intermediaries to take action to restrict content'.[15] They emphasised that:

> [I]ntermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

These international norms are referenced in the Manila Principles on Intermediary Liability, which introduce a framework to assess laws, policies, and practices that govern the liability of intermediaries for third-party content. The Principles state:

> Intermediaries should be shielded from liability for third-party content. Content must not be required to be restricted without an order by a judicial authority. Requests for restrictions of content must be clear, be unambiguous, and follow due process. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality. Laws and content restriction policies and practices must respect due process. Transparency and accountability must be built into laws and content restriction policies and practices.[16]

---

[12] A/HRC/32/38.

[13] A/HRC/32/38, para 43.

[14] A/HRC/32/38.

[15] OSCE, Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda, 3 March 2017.

[16] Manilla Principles on Intermediary Liability.

Data protection

The digital era raises substantial new privacy concerns. The handling of increasingly large amounts of personal data by both state actors and tech companies (and indeed other companies) poses privacy risks. States should therefore enact modern data protection laws which, among other things, require the responsible handling of and prevent inappropriate access to and use of personal data, including by state actors. The rules governing state surveillance should incorporate procedural safeguards, effective oversight, and requirements for authorisation, as well as the possibility of review by independent bodies.[17] Laws which automatically compel data sharing with administrative authorities would not, for example, meet this requirement.

Requirements that private companies retain personal data or store such data within a country ('data localisation' requirements) are also problematic.[18] Such requirements create vulnerabilities and make it more likely that data will be subject to unauthorised access. When paired with legal regimes which make it easy for authorities to access personal data, such rules can seriously undermine the right to privacy and, particularly in authoritarian contexts, pose a serious risk to activists, journalists, human rights defenders, and others who may be targeted for exercising fundamental rights. Laws which prohibit anonymous speech, which is protected under human rights law, raise similar problems.[19] Requiring internet users to register their real identity or provide personal data poses risks to both freedom of expression and privacy.[20]

Human rights and the private sector

Under international human rights law, states have obligations to avoid perpetrating violations of human rights and to put in place a framework for the protection of rights. They are not necessarily responsible for the acts of third parties, such as private companies, but international human rights law does impose certain responsibilities on states towards such actors. This includes the responsibility to put in place legal frameworks which prohibit human rights abuses by third parties and to take action in response to failures to respect those legal frameworks. Specifically, states should 'exercise due diligence to prevent, punish, investigate or redress' harm caused by private actors.[21]

---

[17] A/HRC/39/29, paras 34–35, 39.

[18] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 30 March 2017, A/HRC/35/22, para 20.

[19] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, para 23.

[20] A/HRC/23/40, paras 23, 68–69.

[21] Human Rights Committee, General Comment No. 31, para 8.

States are the primary duty bearers under human rights law, but this includes obligations to regulate and respond to private actors. Companies also have human rights responsibilities, although they do not have obligations in the same manner as states.
A leading reference document outlining these responsibilities is the UNGP's.[22] This is a set of globally recognised guidelines providing a framework for states and businesses to prevent and address the human rights impact of corporate activities. They are based on 3 pillars:

(i) States' duty to protect human rights against abuses by businesses
(ii) Corporate responsibility to respect human rights
(iii) (iii) The duty to provide access to remedies

The first pillar reflects the obligations of states under international human rights law to address human rights abuses by third parties, summarised briefly above. More specifically, the UNGPs affirm that states must take 'appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication'.[23]

The second pillar focuses on the responsibility of companies to respect human rights. This includes both avoiding causing adverse human rights impacts and addressing human rights impacts linked to their operations. Implementing this requires companies to adopt appropriate policies and procedures, and the UNGPs outline 3 main ones:

i. A policy commitment to meeting human rights responsibilities
ii. A human rights due diligence process
iii. Processes to provide redress for any adverse human rights impacts.

Under the third pillar, states have a primary obligation to ensure access to remedies for human rights violations via both judicial and non-judicial mechanisms. However, the UNGPs also affirm that industry and multi-stakeholder initiatives should ensure that effective redress mechanisms are available.

State actors, the private sector, and other stakeholders should ideally work together across all 3 pillars to ensure respect for human rights. However, where states fail in their obligations under the first pillar, or even in their own primary obligations to respect rights, this can be particularly difficult for companies.

---

[22] UNGPs.
[23] UNGPs, Principle 1.A.1.

Principle 23 of the UNGPs affirms that businesses should both comply with applicable laws and respect internationally recognised human rights. Where these conflict, they should 'seek ways to honour the principles' of human rights. This principle affirms that businesses cannot use domestic law as an excuse for disregarding their international human rights responsibilities.

Rather, if the domestic context 'renders it impossible' to fully meet human rights responsibilities, businesses should respect human rights principles 'to the greatest extent possible in the circumstances' and should be able to demonstrate their efforts to do so.

Applying the UNGPs to tech companies raises some particular challenges. The operations of tech companies raise complex jurisdictional issues because they have users potentially in every country in the world. Tech companies also face a large number of complex 'end-use' human rights risks, given the vastly varied uses made of the services they offer. Nonetheless, given that many tech companies provide services which are crucial to the realisation of freedom of expression and access to information, as well as other rights, it is particularly important that both they and states respect human rights in the context of their operations. There are also an increasing number of resources available for applying the UNGPs in the technology context,[24] as well as principles, such as the Santa Clara Principles (endorsed by a number of major tech companies),[25] that outline appropriate company approaches to transparency and accountability in the content moderation process.

These challenges are aggravated in authoritarian contexts where states are failing in their duties under Pillar I of the UNGPs. Resources for companies operating in such situations include the Implementation Guidelines produced by the Global Network Initiative (GNI), a multi-stakeholder initiative designed to help companies respect freedom of expression and privacy when faced with government requests which breach those rights. Members of the GNI include major Western tech companies such as Google, Meta, and Microsoft.

[24] For some examples, see the Global Network Initiative (GNI), Implementation Guidelines for the Principles on Freedom of Expression and Privacy, 2017; OHCHR, B-Tech Project; OHCHR, Report on the Practical Application of the Guiding Principles on Business and Human Rights to the Activities of Technology Companies, 21 April 2022.

[25] The Santa Clara Principles On Transparency and Accountability in Content Moderation. Since 2018, twelve major companies – including Apple, Facebook (Meta), Google, Reddit, Twitter (X), and Github – have endorsed the Santa Clara Principles and the overall number of companies providing transparency and procedural safeguards has increased, as has the level of transparency and procedural safeguards provided by many of the largest companies.

According to the GNI Implementation Guidelines, companies should encourage governments to be 'specific, transparent and consistent' when their demands impact freedom of expression or privacy.[26] They should also adopt policies and procedures for responding to such demands. If required to restrict communications or remove content, they should require governments to follow established domestic legal processes and 'request clear written communication from the government which explain[s] the legal basis' for such requests.[27] Participating companies should also interpret government demands narrowly. If a request appears to be overbroad or inconsistent with domestic or human rights law, companies should seek clarification or modification; seek assistance from relevant authorities, human rights bodies, and NGOs; and challenge the government in domestic courts.[28] Taking such steps can help companies to meet their responsibilities under Principle 23 of the UNGPs.

Using the basic framework of the UNGPs, this report considers the situation in China, Vietnam, and Myanmar. For each country, it provides brief background context and then summarises the main legal obligations placed on tech companies which could implicate them in violations of the rights to freedom of expression and privacy. It then highlights how companies have responded to these requirements, focusing on select case studies. This is used as background for a practical discussion of how the UNGPs can be implemented in highly authoritarian contexts where tech companies face legal requirements which conflict with their human rights responsibilities.

[26] GNI, Implementation Guidelines, Guideline 3.3(a).
[27] GNI, Implementation Guidelines, Guideline 3.2(b).
[28] GNI, Implementation Guidelines, Guideline 3.3.

China

Country context

State control over China's internet infrastructure, maintained since the early days of the internet, has been buttressed by technological measures and legal instruments which enable widespread censorship. For many years, China has asserted a vision of internet sovereignty which asserts its exclusive right to govern the internet within its borders and its citizens' use of that internet; this has only deepened under the country's leader Xi Jinping.[29] Recently, the Chinese Communist Party (CCP) has also been promoting a vision of 'internet civilisation' comprising a 'clean' and harmonious internet which reflects and promotes CCP values.[30]

China imposes extensive blocking and filtering of the internet. Major international tech services are blocked, including social media and messaging services like Facebook, WhatsApp, Twitter, Instagram, YouTube, Telegram, and Snapchat; search engines like Google and Yahoo; and international news outlets like the BBC, the *New York Times*, and Reuters.[31] Between 2017 and 2021, roughly 55,000 active apps, most of which remained available elsewhere, disappeared from Apple's App Store in China.[32] Filters also operate to block content on sensitive issues, such as by preventing users from posting content with certain keywords or hiding such posts.[33]

Because China has incorporated censorship tools into its internet infrastructure, it can impose quite targeted internet disruptions and blocks. Accordingly, it relies less than some of its neighbours on full internet shutdowns. For example, China initially and infamously imposed one of the world's first major internet shutdowns when it blocked internet in Xinjiang Uyghur Autonomous Region for 10 months after Uyghur protests in July 2009.[34] Since then, however, while internet cuts have remained a problem in the region, China has relied largely on a broader range of tactics, including censorship and detention of developers and IT experts, to censor and 'erase' the Uyghur internet.[35] It has deployed a similar combination of tactics in Tibet, such as tailored censorship rules, local law enforcement infrastructure focused on monitoring online content, and arbitrary detentions based on online posts.[36]

---

[29] S. McKune, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, *International Journal of Communication*, 12 (2018), pp. 3835–3855, p. 3837.

[30] *China Daily*, Official Calls for Advancing Cyber Civilization Progress, 29 August 2022; J. Costigan, Determining the Future of the Internet: The U.S.–China Divergence, Asia Society Policy Institute, 19 January 2023.

[31] Freedom House, Freedom on the Net 2023: China.

[32] J. Nicas, R. Zhong, and D. Wakabayashi, Censorship, Surveillance and Profits: A Hard Bargain for Apple in China, *New York Times*, 17 May 2021.

[33] J.Q. Ng, Tracing the Path of a Censored Weibo Post and Compiling Keywords that Trigger Automatic Review, The Citizen Lab, 10 November 2014.

[34] E. Wong, After Long Ban, Western China is Back Online, *New York Times*, 14 March 2010.

[35] M. Borak, The Strange Death of the Uyghur Internet, *Wired*, 2 November 2022.

[36] Human Rights Watch, 'Prosecute Them with Awesome Power': China's Crackdown on Tengdro Monastrery and Restrictions on Communications in Tibet, 6 July 2021.

In addition to its censorship system, China controls the information landscape by promoting pro-government or approved content online. This is done partly via government employees generating mass posts as additional part-time work, but Chinese propaganda departments and individual government agencies also regularly hire private companies to conduct public opinion monitoring and to support influence operations.[37]

Legal obligations on tech companies

China's censorship system functions in part by imposing censorship obligations on tech companies. Companies are expected to impose not only the content prohibitions contained in a range of laws and regulations, but also non-codified political guidelines.[38] China typically enacts laws with intentionally vague or flexible provisions, supplemented by numerous regulations or other directives. This creates a complex and sometimes arbitrary regulatory environment. The remainder of this section outlines some of the most important laws and regulations, but given the complexity of this legal landscape, it is certainly not a comprehensive review.

One of the most important foundational laws for China's current internet regulation is the Cybersecurity Law 2017.[39] Article 9 imposes a very general obligation on network operators to follow laws and regulations, respect social morality, be credible, accept supervision from the government and the public, and bear social responsibility. Article 47 imposes a vague obligation on network operators to strengthen the management of information published by users, and on discovery of prohibited information, 'immediately' stop its dissemination through actions such as deleting it or reporting it.

The Cybersecurity Law refers to the idea of 'critical information infrastructure operators' (CIIOs), but this is not defined clearly. CIIOs can include companies in the information services and telecommunications sectors, but 2021 regulations require precise rules on this to be formulated by relevant industry-specific departments.[40] In practice, it appears that a company receives a notice if it is deemed to be a CIIO.[41]

---

[37] G. King, J. Pan, and M.E. Roberts, How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument, *American Political Science Review*, 111:3 (2017), pp. 484–501; J. Batke and M. Ohlberg, Message Control, *China File*, 20 December 2020.

[38] J. Knockel, K. Kato, and E. Dirks, Missing Links: A Comparison of Search Censorship in China, The Citizen Lab, 26 April 2023.

[39] For an unofficial English translation, see R. Creemers, P. Triolo, and G. Webster, Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), New America, 29 June 2018.

[40] Creemers, Triolo, and Webster, Translation: Cybersecurity Law.

[41] A. Gamvros and L. Wang, 'Am I A CII Operator?' New Regulation Provides More Clarity, Norton Rose Fulbright, 18 August 2021.

China requires data localisation for data or entities operating in certain areas or specialised industries.[42] This represents a fairly expansive data localisation regime, although it is not technically applicable to all internet companies and services as some sources suggest.[43] The Cybersecurity Law imposes certain data localisation requirements on CIIOs, which must also undergo a security assessment before transferring data outside of China.[44] Real-name registration requirements are imposed on mobile phone, domain name registration, and other specified network operators, which must then require users to provide information on their real identity.[45] More generally, network operators must provide technical support and assistance to security authorities.[46] Article 58 also enables authorities to impose temporary measures to limit network communications in a designated area in order to protect national security or to respond to major security incidents.

Along with the Cybersecurity Law, 2 other laws form the core of the data management obligations imposed on companies operating in China. The Data Security Law 2021[47] introduces general data management requirements, such as restrictions on the cross-border transfer of data, and establishes categories of information which are subject to special management rules (such as if the data impacts national security). The Personal Information Protection Law 2021 outlines personal data protection obligations for companies, but with additional elements such as data localisation for CIIOs which handle more than a certain quantity of personal data and mandatory state security assessments prior to cross-border transfers of personal data.[48]

Tech companies are also subject to legal obligations under a range of national security laws, including:

- National Security Law 2015: This important framework law requires enterprises and other organisations to preserve national security, defined broadly to include public welfare and other 'major national interests', and to cooperate with authorities to implement security measures.[49] It also tasks the state with establishing a national network and information

[42] A. Douglas and H. Feldshuh, How American Companies Are Approaching China's Data, Privacy, and Cybersecurity Regimes, The US–China Business Council, April 2022

[43] Freedom House, Freedom on the Net 2023: China; A. Robertson, Facebook Takes a Shot at Apple in China, Says it Won't Store Data in Certain Countries, *The Verge*, 6 March 2019.

[44] Creemers, Triolo, and Webster, Translation: Cybersecurity Law, Article 37.

[45] Creemers, Triolo, and Webster, Translation: Cybersecurity Law, Article 24.

[46] Creemers, Triolo, and Webster, Translation: Cybersecurity Law, Articles 28 and 69.

[47] Creemers, Triolo, and Webster, Translation: Cybersecurity Law.

[48] Creemers and G. Webster, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, unofficial English translation, DigiChina, 20 August 2021, Article 40.

[49] China Law Translate, National Security Law of the People's Republic of China, unofficial English translation, 1 July 2015, Articles 2, 11, and 79.

security safeguard system, preventing and punishing the dissemination of unlawful and harmful information, and maintaining cyberspace sovereignty.[50]

- Counter-Terrorism Law 2015 (amended in 2018): Articles 18 and 19 of this law require telecommunications operators and internet service providers (ISPs) to provide technical support to security authorities to prevent and investigate terrorist attacks; to establish monitoring systems for terrorist content; and to comply with orders to disrupt transmissions, close websites, or delete information in response to terrorist or extremist content.[51]

- National Intelligence Law 2017 (amended in 2018): This law imposes a general obligation on organisations to support, assist, and cooperate with national intelligence efforts and authorises intelligence actors to access communications tools, buildings, and relevant files and materials in the course of their work.[52]

- Counter-Espionage Law 2023: This revised and expanded law grants fairly expansive powers to state security organs to inspect facilities and electronic equipment and to access relevant data in the course of counter-espionage activities.[53]

There are also numerous regulations governing the online space, including the operations of intermediaries. These are too numerous to detail here, but key recent regulations include:

- Provisions on the Governance of the Online Information Content Ecosystem 2019: These provisions consolidate earlier regulations into a more systematic framework of rules.[54] They address 3 types of content: illegal content, defined in broad categories such as endangering national security, undermining honour, or opposing the Constitution; negative content, such as sensational or vulgar content; and encouraged content, such as that which promotes 'Xi Jinping Thought'[55] and other pro-CCP content. Internet users, content producers, and service platforms all have different responsibilities vis-à-vis these types of content. All are also supposed to avoid specified activities, including using networks for illegal conduct such as defamation and threats or registering fake accounts.[56]

---

[50] National Security Law, Articles 25 and 59.

[51] China Law Translate, Counter-Terrorism Law (as amended in 2018), unofficial English translation, 27 December 2015, Article 84.

[52] China Law Translate, PRC National Intelligence Law (as amended in 2018), unofficial English translation, 27 June 2017, Articles 7 and 16–17.

[53] China Law Translate, Counter-espionage Law of the P.R.C. (2023 ed.), unofficial English translation, 26 April 2023, Article 25–26 (among others).

[54] R. Davis, China's New Internet Censorship Rules Outline Direction For Content, *Variety*, 3 January 2020.

[55] For an explanation of 'Xi Jinping Thought', see ARTICLE 19, The Digital Silk Road: China and the Rise of Digital Repression in the Indo-Pacific, 2024, p. 18.

[56] China Law Translate, Provisions on the Governance of the Online Information Content Ecosystem, unofficial English translation, 21 December 2019, Articles 21–25.

- Platforms are specifically prohibited from transmitting content in the 'illegal' category and must prevent and avoid negative content on certain key parts of their platforms. They must also align personalisation algorithms with the content requirements, take action to ensure appropriate use by minors, and strengthen the inspection of advertising.[57] More generally, they must establish rules and systems governing the online content ecosystem, such as systems to register users and review comments.[58] They must also meet certain governance requirements.[59]

- Regulation of Recommendation Algorithms: This 2022 regulation imposes a range of requirements related to recommendation algorithms, such as those used on social media platforms.[60] It requires recommendation algorithms to 'align with mainstream values' and 'promote positive and uplifting activity' by users. Service providers may be classified as having 'public opinion properties or capacity for social mobilisation'. Such companies must provide details to authorities about their algorithms. Based on this regulation, China has compelled major companies to share algorithm data and has established a new algorithm registry. The public version of this registry contains minimal information and provides little insight into companies' actual recommender systems, but it is likely that authorities have access to far more detailed data.[61]

- Provisions on the Management of Internet Post Comments Services 2022: Under these provisions, providers of internet services which enable public commenting or reacting must conduct real-name verification of registered accounts, review any comments for news information before posting, develop systems for managing illegal and negative information, appoint an editorial team to review comments, moderate comments according to user agreements, take action against illegal and negative comments, develop user assessments, and maintain a blacklist of untrustworthy users.[62]

- Provisions on the Management of Internet User Account Information 2022: Over the years, China has imposed various real-identification verification requirements for using online services. These provisions, the most recent iteration, require companies providing

---

[57] China Law Translate, Provisions on the Governance of the Online Information Content Ecosystem, Articles 12–14.

[58] China Law Translate, Provisions on the Governance of the Online Information Content Ecosystem, Article 9.

[59] China Law Translate, Provisions on the Governance of the Online Information Content Ecosystem, Articles 15–17.

[60] R. Creemers, G. Webster, and H. Toner, Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022, unofficial English translation, DigiChina, 10 January 2022; for another version, see China Law Translate, Provisions on the Management of Algorithmic Recommendations in Internet Information Services, 4 January 2022.

[61] A. Liang, Chinese Internet Giants Hand Algorithm Data to Government, BBC, 16 August 2022; M. Sheehan and S. Du, What China's Algorithm Registry Reveals about AI Governance, Carnegie Endowment for International Peace, 9 December 2022.

[62] China Law Translate, Provisions on the Management of Internet Post Comments Services, unofficial English translation, 17 November 2022.

publication or instant messaging services to authenticate users with real identity information. They are supposed to review this information to check for certain prohibited conduct, including posting illegal or negative content as specified in the Provisions on the Governance of the Online Information Content Ecosystem, and to deny service to those found to be in breach. They must also publicly display the location of users' IP addresses.

China's legal framework imposes a direct obligation on tech companies to censor content and requires companies to proactively screen for vaguely defined categories of harmful content. This does not align with human rights standards. The categories of prohibited content are defined far too broadly to align with the 'provided by law' requirement, and many ban legitimate content. China's security laws also require companies to cooperate in a surveillance regime which lacks procedural safeguards and independent oversight and review. While some of its data protection rules require private actors to protect privacy, they also enable state access to that data and lack any protection against misuse of such data by the state. Overall, platforms operating in China will almost certainly be asked to assist in actions which violate human rights law.

Tech company responses

China's highly controlled digital landscape and recent hostility towards large tech companies means that relatively few of the major Western tech companies remain in the Chinese market. Twitter, Facebook, and YouTube have been blocked in China since 2009.[63] Some tech companies, after attempting to engage with the potentially lucrative Chinese market, have exited partially or fully because of the difficult regulatory and political context. The extent to which human rights rather than business concerns drive these exit decisions is not always clear. For example, LinkedIn was able to enter the Chinese market because it censored politically sensitive content and agreed to 2 local firms having an ownership stake.[64] By 2021, it was the only major Western social media platform left in the country and was subject to growing pressure to increase its content censorship. It withdrew its main platform that year, citing the challenging regulatory and operational environment.[65]

Similarly, Google originally agreed to comply with Chinese censorship demands when it launched in China in 2006. In 2010, it was subject to a highly sophisticated hack of Chinese origins, seemingly aimed at accessing the email accounts of Chinese activists. Google then announced that it would no longer accede to censorship demands and relocated its Chinese

---

[63] A. Abkowitz, D. Seetharaman, and E. Dou, Facebook Is Trying Everything to Re-Enter China – and It's Not Working, *Wall Street Journal*, 30 January 2017; L. Hornby and Y. Le, China to Require Internet Domain Name Registration, Reuters, 22 December 2009.

[64] P. Mozur, LinkedIn Said It Would Censor in China: Now That It Is, Some Users Are Unhappy, *Wall Street Journal* (blog), 4 June 2014; P. Mozur and V. Goe, To Reach China, LinkedIn Plays by Local Rules, *New York Times*, 5 October 2014.

[65] P. Mozur, R. Zhong, and S. Lohr, China Punishes Microsoft's LinkedIn Over Lax Censorship, *New York Times*, 18 March 2021; L. McLellan, The Last US-Owned Social Media Platform in China Is Closing, Quartz, 14 October 2021.

search engine to Hong Kong, although China later blocked major Google services.[66] However, in 2018 it emerged that Google was working on developing a China-specific search app which would produce censored results. After public backlash, it dropped the idea.[67]

Meanwhile, China's own tech sector is influential and rapidly growing, including tech giants such as Alibaba, Tencent, and Baidu as well as a strong start-up culture.[68] Chinese tech companies cooperate closely with the PRC government, and there have been recent crackdowns on tech companies deemed to be too powerful. Companies are required to host CCP committees, which have become increasingly assertive.[69] State-owned entities have increasingly bought 'golden shares' in Chinese companies. These typically represent only 1% of shares but are accompanied by a right to a seat on the board of the company and/or veto rights over some key decisions.[70] Overall, information transfer between China's major tech companies and the government is 'comprehensive and systematic', meaning that they are vulnerable to pressure to share data with the government.[71] Chinese tech companies generally score poorly on Ranking Digital Rights' scorecard for how well they protect human rights.[72] Search engine Baidu has at least adopted a human rights policy, and while this is a step in the right direction, it is unusual and the policy is weak, for example qualifying that users' free speech rights will be protected in accordance with national laws and regulations rather than in accordance with international human rights norms.[73]

One of China's most famous home-grown companies, ByteDance, hosts separate apps for its international and Chinese users (Tiktok and Douyin, respectively) in order to comply with domestic Chinese demands while trying to appease users abroad. TikTok now releases transparency reports and has said it will no longer use Chinese-based content moderators for overseas content.[74] Douyin, however, appears to cooperate fully with Chinese government demands. One anonymous former employee has indicated that Douyin has an extensive censorship operation, to which the Cyberspace Administration of China (CAC)

---

[66] Google, A New Approach to China, Official Blog, 12 January 2010; M. Sheehen, How Google Took on China – and Lost, MIT Technology Review, 19 December 2018.

[67] Amnesty International UK, Google: Drop Project Dragonfly, 18 May 2020; J. Su, Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine, *Forbes*, 19 July 2019.

[68] L. Khalil, Digital Authoritarianism, China and COVID, Lowy Institute, 2 November 2022.

[69] J. Horowitz, China to Send State Officials to 100 Private Firms including Alibaba, Reuters, 23 September 2019.

[70] Reuters, Fretting about Data Security, China's Government Expands Its Use of 'Golden Shares', 15 December 2021; P. Frater, Chinese Government Taking Stakes in China's Top Video Streaming Platforms, Says Report, *Variety*, 13 January 2023.

[71] Khalil, Digital Authoritarianism.

[72] Ranking Digital Rights, The 2020 RDR Index, 2020.

[73] Baidu, Baidu Releases Human Rights Policy, Business & Human Rights Resource Centre, 11 November 2020.

[74] TikTok, Government Removal Requests Report, 12 May 2023; Wall Street Journal, TikTok to Stop Using China-Based Moderators to Monitor Overseas Content, 15 March 2020.

issues regular directives, sometimes at a rate of over 100 per day.[75] Since 2021, a Chinese state-owned company has held a golden share in the subsidiary which holds Douyin's licence.[76] Ranking Digital Rights, after attempting to engage with both companies, concluded that ByteDance appears to have a 'hybrid model for handling public criticism', with a Beijing office focused on China and the US and Singapore offices handling TikTok-related matters, although the 'extent to which one informs the other remains unclear'.[77]

Western tech companies which remain in China may increasingly pursue a strategy similar to that of ByteDance. As the following case studies show, however, Chinese operations cannot always be neatly separated from international ones. In addition, acceding to Chinese demands raises difficult questions for Western companies with a claimed commitment to respect human rights.

Case study: Apple in China

Apple is one of the few major Western tech companies which maintains a significant presence in China, alongside Microsoft. China is important to Apple in terms of both manufacturing (Apple assembles most of its products in China) and revenues (in the first quarter of 2023, Apple's revenue from China was almost USD 24 billion, only slightly less than its revenue from the whole of Europe).[78] Apple's Human Rights Policy commits to an approach 'based on the UN Guiding Principles for Human Rights', including following the 'higher standard' where national law and international human rights standards differ and, if they are in conflict, respecting national law while 'seeking to respect' human rights principles.[79] In practice, although Apple has shown signs of attempting to push back on some Chinese requirements, it typically ultimately complies, citing Chinese law.[80]

Apple's history of removing apps from its app store showcases this approach. China has long required all websites in China to apply for an Internet Content Provider Filing Number. In 2016, it required online games to obtain this licence as well. Apple managed to delay implementation of this requirement, which was enforced by Android stores owned by Chinese companies, apparently by exploiting some loopholes in the rules. However, in 2020

[75] S. Lu, I Helped Build ByteDance's Censorship Machine, *Machine Learning Times*, 18 February 2021.

[76] Y. Yang and B. Goh, Beijing Took Stake and Board Seat in Key ByteDance Domestic Entity This Year, Reuters, 17 August 2021.

[77] J. Zhang, Why Won't Chinese Companies Talk to Us? It's Complicated, Ranking Digital Rights, 2022.

[78] F. Laricchia, Revenue of Apple by Geographical Region from the First Quarter of 2012 to 3rd Quarter 2023, Statista, 17 May 2024.

[79] Apple, Our Commitment to Human Rights, 2020.

[80] For more on Apple's actions in China, see M. Caster, Blog: Apple Says It Cares about Digital Rights. Unless You're in China, ARTICLE 19, 13 July 2021.

Apple purged non-compliant apps following an apparent crackdown by Chinese authorities.[81]

As of 2023, China requires all apps to obtain this licence (among other requirements). Apple staff had a series of discussions with Chinese officials to express concerns about the rule but, as of October 2023, Apple began to implement it.[82] This is a significant development because users have long used the Apple's App Store to gain access to apps which are otherwise blocked in China, such as Instagram, YouTube, and WhatsApp; users have been able to download them and then use a VPN to access them.[83]

Beyond enforcing these general licensing requirements, Apple has also long faced criticism for removing apps deemed to be politically sensitive in China, often in a non-transparent way. For example, a 2021 *New York Times* analysis noted that Apple's own figures indicated that they had removed 1,217 apps in 2018–2020, approving 91% of the government's requests, while removing only 253 apps in all other countries combined (representing 40% of removal requests). [84] The *Times* estimated that this number was low, since 55,000 apps had disappeared from the store since 2017. Apple contested these figures, arguing that many developers had removed the apps of their own accord. However, the *Times* attributed at least some of the difference to Apple internally censoring apps even absent a takedown request.

A former head of Apple's App Store who said that Apple's lawyers in China gave his team a list of forbidden topics, such as 'Tiananmen Square', and that associated apps were then removed proactively.

A Tech Transparency Project report reached similar conclusions, identifying 3,200 missing apps in a six-month period compared with only hundreds which were reported by Apple. Although, again, these missing apps could have been voluntarily removed by developers, the Tech Transparency Project concluded there was likely additional censorship by Apple of apps with sensitive content such as human rights, religion, politics, and LGBTQI+ issues,

[81] J. Porter, Apple Closes Chinese App Store Loophole, Causing Thousands of Games to be Removed, *The Verge*, 22 June 2020; Al-Jazeera, Game Over: Apple Removes Thousands of Titles from China App Store, 15 July 2020.

[82] Y. Kubota, Y. Jie, and A. Tilley, Apple's Latest China Challenge: A Crackdown That Could Shrink Its App Store, *Wall Street Journal*, 29 September 2023; Apple Developer, Reference: App Information; W. Davis, Apple Is Locking Down the iPhone App Store to Comply with a New Law in China, *The Verge*, 3 October 2023.

[83] Kubota, Jie, and Tilley, Apple's Latest China Challenge.

[84] Nicas, Zhong, and Wakabayashi, Censorship, Surveillance and Profits.

given the complete absence of such apps.[85] The report also identified 330 missing VPN apps. Apple began removing VPN apps from its stores in 2017 in response to new laws which required all VPN providers to obtain a government licence, stating that it had been required to remove apps which did not meet new regulations.[86]

Apple has also made other changes in apparent response to Chinese pressure, even without a specific legal requirement to do so. When protesters were using Apple's AirDrop file-sharing feature in 2022, Apple introduce a feature limiting file sharing with strangers to a 10-minute period. Eventually, in June 2023, CAC proposed draft regulations restricting wireless file-sharing services like AirDrop, but Apple's 2022 action appeared to be in response to Chinese pressure or on its own initiative, rather than in response to a legal requirement.[87]

Apple has also increasingly acceded to Chinese demands in the privacy realm, despite cultivating an image as a privacy champion in the West.[88] In 2017, Apple relocated data of Chinese customers to servers inside China, apparently in response to new legal requirements in the Law on Cybersecurity.[89] At the time Apple claimed that it retained access to encryption keys in order to protect the locally stored data, but it subsequently acknowledged that Chinese iCloud decryption keys would be stored in China.[90]

Apple also shares data with Chinese authorities upon request so as to comply with Chinese law. This potentially creates a conflict with its obligations under US law, which prohibit American companies from sharing data with Chinese law enforcement actors. To reconcile these obligations, Apple ceded legal ownership of customer data in China to GCBD (Guizhou-Cloud Big Data), a Chinese company. Requests for the data of Apple's customers in China are now made by the Chinese Government to GCBD, meaning that Apple is technically not the entity providing the data.[91] Apple's own information notes that in the first half of 2022, it received 1,481 individual requests for user data, relating to information for 167,854 different devices and accounts; Apple provided data for 95% of these requests.[92]

---

[85] Tech Transparency Project, Apple Is Censoring Its App Store for China, 23 December 2020.

[86] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Letter to Tim Cook, 4 August 2017.

[87] W. Chan, Why Is Apple Limiting Chinese Protesters' Use of AirDrop?, Fast Company, 29 November 2022; R. Cheung, China Plans New Rules to Regulate File Sharing Services Like Airdrop and Bluetooth, *Guardian*, 9 June 2023.

[88] K. O'Flaherty, Apple Slams Facebook and Google with Bold New Privacy Ad, *Forbes,* 25 May 2022.

[89] Nicas, Zhong, and Wakabayashi, Censorship, Surveillance and Profits.

[90] Caster, Apple Says it Cares about Digital Rights.

[91] O'Flaherty, Apple Slams Facebook and Google.

[92] Apple, China Mainland: Transparency Report, July–December 2022.

Apple's shareholders have organised some pushback in response to its conduct in China. The company released its Human Rights Policy, cited earlier, after shareholders voted on a proposal for greater transparency over China's attempts to restrict freedom of expression on Apple products; the proposal, initiated partly by a non-profit organisation, failed but garnered 40% of shareholder votes.[93] Shareholder advocacy in the tech company context can be challenging because of the nature of the share structure of most tech companies, but it has increasingly been used as an advocacy tool and may be an effective tactic in a country like China with a highly restrictive civic space.[94]

Case study: Microsoft's Bing in China

Microsoft's search engine Bing remains active in the Chinese market and even overtook domestic search engines as the top search engine in China in 2023.[95] It has been able to stay in the Chinese market because it has complied with Chinese censorship demands.

Bing has declined to discuss its policies in China but it does censor content that the government considers sensitive in its search results in China.[96] In early 2023, the Citizen Lab published a study comparing the levels of censorship across 8 of the major search platforms accessible in China.[97] It found that Bing search results demonstrated higher rates of censorship in terms of political and religious content than those of Chinese counterparts, including Baidu, the dominant Chinese search engine.[98] The study cast serious doubt on the theory that foreign companies offer less-censored services.

Limited information is available about the extent to which Microsoft may be negotiating or pushing back. There have been signs of crackdowns on Microsoft by authorities at various points. In July 2014, 4 of its offices in China were raided by officials, who questioned

[93] Tech Transparency Project, Apple Is Censoring Its App Store for China; Eko, 40% of Shareholders Defy Apple Management in Vote on China Cyber Surveillance, 26 February 2020.

[94] J. Rydzak, Dissecting Big Tech's Shareholder Showdown, Ranking Digital Rights, 16 June 2022; A.L. Nabors, Is Momentum on Tech Shareholder Activism Stalling? How to Reinvigorate It in 2024, Ranking Digital Rights, 5 July 2023.

[95] A. Hasnain, Microsoft Bing Emerges as China's Favorite Search Engine, Digital Information World, 24 May 2023.

[96] T. Simonite, US Companies Help Censor the Internet in China, Too, *Wired*, 3 June 2019.

[97] Knockel, Kato, and Dirks, Missing Links.

[98] Knockel, Kato, and Dirks, Missing Links.

executives and downloaded data from the company's servers.[99] In 2019, Bing was temporarily blocked in China on the same day the authorities announced that they had closed 733 websites and shut down 9,382 apps in a crackdown on 'harmful' information. When Microsoft confirmed that Bing had been temporarily inaccessible, Microsoft's president Brad Smith said that Microsoft had 'days when there are either difficult negotiations or even disagreements' with the Chinese authorities about search results on Bing but that Microsoft was 'not aware of any ongoing negotiation or disagreement, so we're working to understand it better'.[100] In 2021 and again in 2022, Bing said that it had been required by regulators to temporarily suspend its autosuggest feature. No reason for the suspension was given.[101]

For many years, there has been evidence that Bing has censored searches. In 2009, searching for terms such as 'Tiananmen' on Bing in English or traditional Chinese produced results about 'killings', but searches in simplified Chinese produced 'sanitized pro-communist results'.[102] Microsoft denied that it was censoring search results, claiming it was a bug which was being fixed, but 6 months later these searches were still being censored.[103]

At times, censorship of political topics in China appears to impact Bing search results even outside of China. In 2014, searches in the United States generated different results in simplified Chinese than in English, apparently due to censorship of controversial topics such as the Dalai Lama or the Tiananmen Square protests. Bing blamed an error in its system.[104] One expert suggested that Microsoft was not intentionally censoring results internationally but was engaging in 'second hand censorship' by failing to consider the impact of applying its normal search algorithms in the censored Chinese information landscape.[105] In any case, Bing seems to have failed to address the problem. In 2021, search results for 'Tank Man' failed to produce the iconic image of the protester in Tiananmen Square, including for international users.[106] A more comprehensive study in 2022 by the Citizen Lab also found that the autosuggest feature in the United States and Canada exhibited signs of politically sensitive results being censored in China. The authors hypothesised various reasons for this but ultimately concluded that it was not possible for the platform to insulate its operations outside of China from censorship that it was enforcing inside China.[107]

---

[99] P. Mozur and K. Weise, China Appears to Block Microsoft's Bing as Censorship Intensifies, *New York Times*, 23 January 2019.

[100] S. Pham, Microsoft Search Engine Bing Was Briefly Blocked in China, CNN, 24 January 2019.

[101] Reuters, Microsoft's Bing Suspends Auto Suggest Function in China at Government's Behest, 17 December 2021; Reuters, China Requires Microsoft's Bing to Suspend Auto-Suggest Feature, 21 March 2022.

[102] N. Kristof, Microsoft and Chinese Censorship, 24 June 2009, *New York Times Opinion*.

[103] Kristof, Microsoft and Chinese Censorship.

[104] D. Rushe, Microsoft Blames 'System Error' but Denies Censoring Chinese Search Results, *Guardian*, 12 February 2014.

[105] Rushe, Microsoft Blames 'System Error'.

[106] BBC, Microsoft Says Error Caused 'Tank Man' Bing Censorship, 5 June 2021; M. Caster, Opinion: Big Tech Needs a Reset on Chinese Censorship, Thomson Reuters Foundation News, 7 June 2021.

[107] J. Knockel and L. Ruan, Bada Bing, Bada Boom: Microsoft Bing's Chinese Political Censorship of Autosuggestions in North America, The Citizen Lab, 19 May 2022.

Vietnam

Country context

Vietnam's censorship and surveillance apparatus is nowhere near as comprehensive as China's, but the government appears to have ambitions to develop a similar system. In the meantime, it still has fairly sophisticated technical surveillance capacity and, combined with offline surveillance and arrests and imprisonment of critics, the country presents a highly repressive environment for freedom of expression.

The government controls the telecommunications infrastructure in the country, which is mostly in the hands of state- and military-owned telecommunications companies, giving it the power to restrict access to the internet. Vietnam has engaged in tactics such as throttling internet access during protests and prominent trials and slowing Facebook services in an effort to compel Meta to increase content removal.[108] Foreign media websites and websites hosting political or human rights content are also routinely blocked in the country. One study documented more than a thousand inaccessible websites, more than half of which were hosting political criticism or news media, during the first half of 2022.[109] Government ministries themselves report blocking thousands of websites annually.[110]

Where it cannot technically control content, Vietnam uses human beings to monitor social media and attempt to shape the online narrative. In 2017, the Vietnam military announced the formation of a 'Force 47' division, supposedly incorporating 10,000 'cyber-troops' responsible for promoting pro-government content.[111] Parallel citizen volunteer units of 'opinion shapers' also exist, although the precise relationship of these groups to government entities is unclear. Because Vietnam lacks the resources that China has to exercise absolute control over the internet, it has instead used 'public opinion shapers' to control public perceptions of the government through, in part, maintaining a strong presence in the comments section of social media accounts and flooding pages with pro-government messages to create the illusion of support.[112] These monitors also target or harass critics and activists, both online and by reporting them to the police.[113]

Vietnam also uses the criminal law as a censorship tool. Amnesty International has said that more than 40% of prisoners of conscience in Vietnam (as of 2020) were imprisoned solely for their social media use.[114] Vietnamese activist organisation the 88 Project counted 178

---

[108] M. Caster, Vietnam: Confronting Digital Dictatorship, ARTICLE 19, 12 September 2023.

[109] Independent researchers (anonymous), K. Koh, and S.N. Samsudin, iMAP State of Internet Censorship 2022 – Vietnam, OONI, 23 December 2022.

[110] Freedom House, Freedom on the Net 2022: Vietnam and Freedom on the Net 2023: Vietnam (both citing Vietnamese-language government sources).

[111] J. Pearson, Insight: How Vietnam's 'influencer' Army Wages Information Warfare on Facebook, Reuters, 9 July 2021.

[112] Viet Tan, #StopVNtrolls: Combatting Force 47 and Cyber Censorship, 30 January 2023.

[113] S. Biddle, Facebook Lets Vietnam's Cyberarmy Target Dissidents, *The Intercept*, 21 December 2020.

[114] Amnesty International, Viet Nam: Tech Giants Complicit in Industrial-Scale Repression, 1 December 2020.

activists in prison in October 2023, commonly due to charges under Articles 117 and 331 of the Penal Code.[115] These articles can result in multi-year prison sentences for sharing distorted information about the government or abusing freedom of speech or other freedoms to infringe on the interests of the state.[116] Such provisions represent a serious breach of human rights standards and can easily be used to silence dissent. In practice, they have often been used against journalists, activists, and bloggers for their online posts.[117]

Legal obligations on tech companies

Vietnam relies on private companies to aid its online censorship efforts. It has enacted a number of laws which place obligations on tech companies to moderate or remove content and share data with authorities. Important new draft laws and regulations are currently under development:

- Decree 72/2013 (and a draft replacement decree): This wide-ranging decree is one of the most important Vietnamese legal instruments for regulating the internet. It imposes intermediary liability and other obligations on certain classes of service providers. For example, 'aggregated information websites' and companies providing social networks must establish at least one server in Vietnam to enable the provision of data to authorities, must avoid disseminating prohibited content, and must remove prohibited content at the request of authorities.[118]

  Subsequent regulations have elaborated further on the requirements in Decree No. 72. However, at the time of writing, a draft decree to replace Decree No. 72 is under discussion. Among other things, this would require social media users to authenticate their accounts with personal information and require platforms to screen content proactively and comply with 24-hour takedown notices.[119]

- Law on Cybersecurity, 2019 (LCS): The LCS imposes a number of obligations on service providers and 'system administrators', which must remove specified prohibited content at the request of a 'cyber task force' created by the LCS.[120] System administrators are also required to take action to detect and block the sharing of state secrets and other confidential information, such as business and private secrets.[121] Websites and portals

---

[115] The 88 Project, Database of Persecuted Activists in Vietnam.

[116] Penal Code, No. 100/2015/QH13, 27 November 2015, English translation.

[117] OHCHR, Viet Nam: Arrests Send Chilling Message before Key Party Meeting – UN Experts, 14 January 2021.

[118] Articles 24–25. The requirements are slightly different for each category. Aggregated information websites appear to have a stronger obligation to screen for and remove prohibited content, while social networks must avoid providing it.

[119] Caster, Vietnam: Confronting Digital Dictatorship; Global Network Initiative, GNI Submission to the Government of Vietnam on Potential New Decree 72 on the Management, Provision and Use of Internet Services and Online Information, 2023.

[120] Law on Cybersecurity, No. 24/2018/QH14, 12 June 2018, English translation, Articles 16(6) and 26(2).

[121] Law on Cybersecurity, Article 17(2).

must not provide or transmit certain types of content, including anything which infringes on national security.[122] None of these requirements are very clear in the absence of implementing regulations, but overall they provide a legal framework for imposing intermediary liability.

Article 26 also requires service providers to authenticate user data upon registration and to provide user information to the Ministry of Public Security on request to aid in investigating LCS violations. Other provisions grant fairly intrusive inspection powers to a cyber task force in the Ministry of Public Security, including to inspect information stored on information systems. There is a data localisation requirement for foreign companies handling the personal data of Vietnamese citizens, which must also have a branch or office in Vietnam.

- Decree 53/2022: This is a crucial implementing decree for the LCS. It sets out a 'triggering' provision for the requirement to store data locally; if foreign companies do not comply with the Vietnamese Government's request for content removal and the sharing of users' data, the government can order the company to localise the data and open a local branch, which they must do within 12 months.[123] Domestic companies have more immediate obligations to implement local data storage for certain kinds of data (primarily the personal data of Vietnamese citizens). Decree 53 also empowers administrative authorities to initiate enforcement actions in response to illegal content, such as by issuing takedown notices, requesting a system shutdown or suspension of domain names, or requiring information disclosure and inspection.[124] It also allows the Ministry of Public Security to suspend or terminate a range of apps and websites.

- Vietnam has indicated that it is enacting other measures too. For example, it is amending its Telecommunications Law, with a reported change being to mandate social media users to verify their identity.[125] In 2022, Reuters reported that Vietnam was also developing a law requiring social media companies to take down illegal content within 24 hours and block illegal live streams within 3 hours.[126] Some sources suggest that such a requirement was then enacted,[127] but it appears that it has instead been incorporated into the draft decree which will replace Decree 72.[128]

Vietnamese law empowers authorities to order content removal, restrict services, or access personal data without the kinds of protections demanded by human rights standards. For

---

[122] Law on Cybersecurity, Article 26.

[123] PwC, Decree 53 Guiding Cybersecurity Law, PwC Vietnam Legal NewsBrief, 8 September 2022.

[124] KPMG, Legal Alert, September 2022. An English translation of this Decree could not be located.

[125] Reuters, Vietnam to Require Social Media Users to Verify Identity, 9 May 2023; BBC, Vietnam to Crack Down on Anonymous Social Media Accounts, 9 May 2023.

[126] Reuters, Vietnam to Require 24-Hour Take-Down for 'False' Social Media Content, 4 November 2022.

[127] BBC, Vietnam to Crack Down.

[128] Baker McKenzie, Vietnam: Updated Amendments that Affect Internet Services, Client Alert, August 2021.

example, takedown notices are not issued by a court or independent body, and certain intermediaries are expected to screen actively for illegal content. The data localisation and user authentication requirements also raise privacy concerns, particularly when paired with expansive government authority to compel access to that data. Vagueness in the laws, although a serious concern from a human rights perspective, has sometimes allowed companies to resist implementation (as demonstrated in the next section) but also creates confusion as to the exact legal obligations imposed on companies.

Tech company responses

Foreign tech companies, facing increasing pressure from the Vietnamese Government, appear largely to be complying with government content removal demands. Google and Facebook both report data on takedown requests (for Google, these relate to YouTube), and both show sharp increases in requests since 2017. The Vietnamese Government repeatedly claims that the rate of requests accepted by Google and Facebook is high, at 95% and 90% respectively in 2020, for example.[129] Google's own data appears to confirm this, with most requests being related to content containing 'government criticism'.[130] Facebook's situation is similar, as discussed in the case study below.

Amnesty International has said that by complying with so many takedown requests, Facebook and Google 'play an increasingly prominent and complicit role in the Vietnamese authorities' systematic repression of freedom of expression online' and say that both companies are largely deferring to local law without attempting to object to or contest the requests.[131]

Vietnam also completed an investigation into TikTok in 2023, claiming that it violated local laws, including by failing to block content. TikTok indicated that it would remain 'non-political' when it entered the Vietnamese market but has nonetheless faced government pressure following a surge of political content on the platform.[132] After the investigation concluded that TikTok was failing to comply with legal requirements, government sources claimed that

[129] Freedom House, Freedom on the Net 2021: Vietnam. See also a government claim that three platforms had response rates of over 90% to government removal requests in 2023: Tuoi Tre News, TikTok Signs Document to Admit Wrongdoing in Vietnam, 1 July 2023.

[130] Google, Transparency Report, Government Requests to Remove Content, indicates that it complied with most of the 848 requests to block 31,626 items of content which it received from January 2021 to December 2022).

[131] Amnesty International, *Vietnam: Let Us Breathe! Censorship and Criminalization of Online Expression in Viet Nam*, 30 November 2020.

[132] L. Le, Vietnam Pressures TikTok to Censor More Content or Face a Ban, *Rest of World*, 24 May 2023; F. Potkin, TikTok Booms in Southeast Asia as It Picks Path through Political Minefields, Reuters, 28 August 2020.

TikTok had agreed to strengthening child protection measures and to 'coordinating communication efforts' with the government, but that it had not agreed to allow Vietnamese legal entities to address content violations according to government requests, citing a lack of Vietnamese legal regulations on this point.[133] If this is accurate, TikTok may be negotiating to some degree over new requirements, but overall it can be expected to comply, given that its content moderation was 'already more localised than that of other social media platforms'.[134] TikTok itself said in a statement that it would 'respect local laws and regulations' and would continue to collaborate with relevant authorities.[135]

TikTok is particularly vulnerable to government demands because it has established a local office – a step major Western social media companies have so far resisted, partly due to concerns over government arrest or intimidation of local employees.[136] Netflix, however, is set to open a local office soon, following a new 2022 rule requiring video-on-demand services to obtain a local licence and open a local office. Amazon Prime Video has since exited the country, presumably to avoid complying with this requirement.[137] If Vietnam is aggressive in implementing the local office requirement for other companies – a possibility following Decree 53/2022 – it may similarly force them to choose between compliance and exit.

Tech companies are also subject to indirect pressures via advertisers. In 2019, the Ministry of Information and Communications said that it had sent letters to 100 local and foreign brands warning them to stop advertising next to anti-state content on YouTube.[138] More recently, following regulations which tightened advertising rules, Vietnam drafted an optional whitelist and mandatory blacklist of sites which can and cannot receive advertising revenues based on whether they have posted 'illegal' content.[139] Advertisers have pulled advertisements in response to these measures, creating added commercial incentives for tech companies to remove content that the government finds objectionable. Google and Facebook have agreed to comply with at least some advertising-related demands, although detailed information on this is not publicly available.[140]

---

[133] VietnamNet Global, Vietnam Urges TikTok to Rectify Its Violations in Vietnam, 8 December 2023 (citing the deputy director of the Authority of Broadcasting, Television and Electronic Information).

[134] Le, Vietnam Pressures TikTok.

[135] N. Quynh, Vietnam Says TikTok's Content Censorship Isn't Effective: Media, BNN Bloomberg, 5 October 2023.

[136] F. Potkin and P. Nguyen, Exclusive: Netflix Making Preparations to Open Vietnam Office, Reuters, 24 February 2023; Le, Vietnam Pressures TikTok.

[137] Potkin and Nguyen, Netflix Making Preparations; L. Quy, Amazon Prime Video to Leave Vietnam, *VN Express*, 16 October 2023.

[138] J. Reed, Vietnam Tells Companies Not to Advertise on YouTube Videos, *Financial Times*, 12 June 2019; AFP, Vietnam Warns YouTube Advertisers over Anti-State Channels, *France 24,* 25 June 2019.

[139] Y. Seck, Vietnam: White List for Online Advertising Services Released, Baker McKenzie, 23 March 2023; L. Hoang, Vietnam to Block Ads on 'Toxic' Online Content in Further Crackdown, Nikkei Asia, 9 December 2022.

[140] Freedom House, Freedom on the Net 2023 (citing Vietnamese sources).

Finally, as mentioned earlier, state actors such as Force 47 and civilian counterparts have become skilled at abusing content moderation systems by flagging legitimate content as violating a platform's rules in an attempt to have the user's account suspended or the content removed.[141] In general, tech companies seem to be struggling with how to respond to this. Meta's reaction is discussed in the following case study.

Case study: Facebook in Vietnam

In Vietnam, Meta is increasingly facilitating censorship and complying with government demands to silence criticism on its platform. Meta's transparency data shows that for the 30 months between January 2020 and June 2022, it removed 6,039 pieces of content at the request of the Vietnamese Government, including posts, pages, groups, and profiles.[142] Although Meta receives a large number of content removal requests from Vietnam, this is fewer than from other countries in the region, likely because Vietnam has so effectively mobilised aggressive mass campaigns to use Meta's own reporting features against groups or individuals who criticise the government.[143] Removals linked to these campaigns would not be accounted for in Meta's transparency reporting.[144]

Meta reports that the removed content referenced in its transparency data was restricted because the government claimed that it violated local laws on slander and insult under Decree No. 72/2013, spreading COVID-19 misinformation, and opposing the Communist Party and Government of Vietnam. As such, Meta itself acknowledges it is complying with content takedown requests which clearly do not align with international human rights law. This explanation is given on a summary basis without any additional details about the nature of the removal requests.

Unofficially, Meta may also be facilitating freedom of expression violations. A 2023 *Washington Post* article quoted 2 anonymous former employees who claimed that Facebook had a private list of Communist Party officials who should not be criticised on the platform. Meta did not respond to the *Post*'s inquiries on this point, except to say that its focus was on ensuring as many Vietnamese as possible could use the platform to express themselves.[145]

Vietnam is of particular significance to Meta; since 2016, it has become one of Facebook's biggest growth markets, representing its seventh-largest user base globally and providing

---

[141] D. Keeton-Olsen, The Vietnamese Military Has a Troll Army and Facebook Is Its Weapon, *Rest of World*, 8 May 2023.

[142] Meta Transparency Center, Content Restrictions Based on Local Law.

[143] Keeton-Olsen, The Vietnamese Military Has a Troll Army.

[144] Biddle, Facebook Lets Vietnam's Cyberarmy Target Dissidents.

[145] R. Tan, Facebook Helped Bring Free Speech to Vietnam: Now it's Helping Stifle It, *Washington Post*, 19 June 2023.

nearly USD 1 billion of annual revenue.[146] Meta therefore has significant business incentives to comply with government demands.

However, the Vietnamese Government has also specifically targeted Facebook. Vietnam slowed Facebook services for around 7 weeks in 2020 by taking its servers offline, although state media claimed the problem was undersea cable maintenance. The servers were restored only after Facebook committed to censoring more anti-state content – according to Reuters, citing internal company sources.[147] Following this incident, Facebook's approach of relative 'caution' in complying with censorship demands shifted to one of 'near-guaranteed compliance', according to claims by the Vietnamese Government.[148]

Facebook admits that it agreed to significantly increase censorship of 'anti-state' posts following this event, saying 'we have taken this action to ensure our services remain available and usable for millions of people in Vietnam'.[149] Amnesty International said that this was possibly the first time that Facebook had officially acknowledged a policy to increase compliance with censorship of political expression at the request of the government, even though such speech is protected under international human rights law.[150] In a letter to Amnesty, Facebook said that it was committed to the UNGPs and referenced Principle 23's language regarding situations where legal obligations and international human rights principles conflict. It also said that its teams only restrict content when it is alleged to be illegal and that their review considers the impact of the decision on the accessibility of speech on its platform.[151]

Facebook therefore sometimes cites the need to remain in the Vietnamese market and at other times the UNGPs. Overall, however, it has provided limited information on the extent to which it complies with Vietnamese laws or applies human rights considerations in its content moderation. It has also not clearly demonstrated that it is respecting human rights to the 'greatest extent possible' given the Vietnamese circumstances.

In terms of blocking users who are misusing the self-reporting feature, in 2021 a Facebook source said that it had removed a private Facebook group called 'E47' whose members were coordinating to report activists.[152] However, it does not appear to have taken strong action against the broader problem of coordinated inauthentic behaviour and mass reporting

---

[146] S. Strangio, Could Vietnam Really Shut Down Facebook? *The Diplomat*, 23 November 2020.

[147] J. Pearson, Exclusive: Facebook Agreed to Censor Posts after Vietnam Slowed Traffic – Sources, Reuters, 21 April 2020.

[148] D. Luong, Meta Cozies Up to Vietnam, Censorship Demands and All, Coda, 28 September 2023.

[149] Pearson, Facebook Agreed to Censor Posts.

[150] Amnesty International, *Let Us Breathe!*, p. 30.

[151] Amnesty International, *Let Us Breathe!*, p. 30.

[152] J. Pearson, Facebook Says It Removes Accounts Which Targeted Vietnamese Activists, Reuters, 1 December 2021.

targeting Vietnamese activists on its platform.[153] One challenge is that individual users engaging in this behaviour do not always hide their identity, so they may not be obviously violating Facebook policy related to inauthentic accounts.[154]

Meanwhile, Vietnamese activists report difficulties in contacting Facebook about unfairly frozen accounts. A Vietnamese advocate who helps users dispute reported community standards violations arising from mass campaigns has said that appealing such decisions to Facebook is a 'slow and difficult process'. He eventually connected with a Meta human rights manager in the United States who could intervene to restore individual posts but contends that Facebook has not acted to address the matter more systematically, stating: 'We hope that someday we can discuss directly with the Facebook team'.[155] Another activist who had been invited to meet with Facebook in 2018 says that she stayed in contact with Meta's human rights team to alert them when accounts of activists were frozen but responses 'slowed and then stopped entirely', and she rarely tries any more.[156]

Case study: Data localisation in Vietnam

The tech industry has actively lobbied against data localisation in Vietnam. In December 2018, just before the Cybersecurity Law came into effect, tech industry association the Asia Internet Coalition sent a letter to the Vietnamese Government criticising the data localisation requirement and its potential harm to economic growth.[157] The letter followed an initial draft of an implementing decree which was ultimately withdrawn and instead became Decree 53/2022/ND-CP, described above.[158] While this lobbying did not succeed in removing a data localisation requirement altogether, Decree 53 did soften the requirement compared with the earlier draft decree. For foreign companies, local data storage is required only on request and is subject to the condition that the company has refused to comply with other government requests.

Since Decree 53 was enacted, the tech industry has continued to lobby against the requirement. The Asia Internet Coalition, along with the US Chamber of Commerce and the American Chamber of Commerce Vietnam, sent another letter to the government in September 2022, asking for clarification on several ambiguous provisions in the decree, including the process for triggering the data localisation requirement and greater precision

[153] Viet Tan, Open Letter Calling on Facebook to 'Unfriend' Harmful Social Networks in Vietnam, 1 February 2023.

[154] Biddle, Facebook Lets Vietnam's Cyberarmy Target Dissidents.

[155] Keeton-Olsen, The Vietnamese Military Has a Troll Army.

[156] Tan, Facebook Helped Bring Free Speech to Vietnam: Now it's Helping Stifle It.

[157] J. Reed, Google and Facebook Push Back on Vietnam's Sweeping Cyber Law, *Financial Times*, 13 December 2018.

[158] M. Nguyen, Exclusive: Vietnam Cyber Law Set for Tough Enforcement Despite Google, Facebook Pleas, Reuters, 10 October 2018.

around the scope of the requirement.[159] In the meantime, we are not aware of any case under Decree No. 53 where Vietnam has demanded that a specific foreign tech company localise data. However, Amazon, at least, is reportedly planning a 'local zone' server which will host a 'fraction' of its operations, with the localisation requirement cited as a factor in these plans.[160]

This example suggests that coordinated lobbying by tech companies can have some impact, at least in terms of delaying or mitigating legal requirements which have negative consequences for human rights. The focus on the economic costs of data localisation may have been particularly impactful, as these could be substantial: one report suggests that data localisation could reduce Vietnam's GDP by 1.7%.[161]

On the other hand, Vietnam may yet order compliance with the data localisation requirements in Decree No. 53, the threat of which will likely be a convenient tool for compelling compliance in other areas, such as content moderation.

In any case, according to tech companies' own numbers, the Vietnamese Government is not making large numbers of formal requests for user data. Facebook reports indicate that from 2015 to 2022, the government made 61 requests. Facebook provided some data for only 18 of them.[162] Google's data shows that from 2014 to 2021, it received 6 requests for data; Apple received 4 requests for user data in 2020 and 2021.[163]

Despite these low numbers, there have been examples in Vietnam of arrests of social media users for anonymous posts, and it is not clear how authorities linked the anonymous accounts to the actual users.[164] Vietnam is known for its relatively sophisticated offline and online surveillance, and it may have sufficient other tools at its disposal to identify such accounts, rendering formal requests to the platform unnecessary. Unfortunately, limited transparency on the topic has made it hard to ascertain how Vietnam is conducting surveillance and accessing personal data. Data localisation would make this easier. To the extent that major tech companies have resisted localisation so far, this may represent a positive example of tech company resistance to domestic laws that compromise human rights.

[159] US Chamber of Commerce, American Chamber of Commerce Vietnam, and Asia Internet Coalition (2022), Letter Re: Decree No. 53/2022/ND-CP detailing the implementation of a number of articles of the Law on Cybersecurity (LOCS), 9 September 2022.

[160] L. Hoang, Amazon Woos Cloud Clients as Vietnam Floats Onshore Data Rules, Nikkei Asia, 11 July 2022.

[161] Hinrich Foundation, CIEM, and AlphaBeta, *The Data Revolution: How Vietnam Can Capture the Digital Trade Opportunity at Home and Abroad*, 2023.

[162] Meta Transparency Center, Government Requests for User Data, 2017.

[163] Apple, Vietnam. Transparency Report: Government Requests, 2021.

[164] Radio Free Asia, Vietnam Arrests Facebook User for Posts Criticizing COVID-19 Policies, 6 October 2021.

Myanmar

Country context

In a February 2021 coup, Myanmar's military overthrew the elected government, reversing almost a decade of fragile democratic reform. Pre-publication censorship had been abolished in 2012, and this was followed by a period of expansion in the media and information landscape. Use of ICT services also exploded with liberalisation and the opening of the telecommunications sector to private and foreign investor.[165] Democratic reforms were modest, however, and freedom of expression challenges remained.

After the 2021 coup, the military could not easily regain the tight control of the information space which it had enjoyed prior to the process of democratisation. Instead, it turned to a range of oppressive measures to suppress dissent. Civic space has become highly constrained and the military is quick to bring criminal charges against anyone who expresses opposition to it or to military rule. As of October 2023, the Assistance Association for Political Prisoners had verified more than 25,000 arrests related to the military's seizure of power since the coup.[166] Courts now rubber-stamp military-supported prosecutions. Martial law is in force in several regions, enabling civilians to be tried in military courts and sentenced to death or life imprisonment for a range of crimes, including mere speech offences like spreading false news.[167] Violent suppression by the military of opposition protests has also accelerated broader armed conflict across Myanmar, and the country is now experiencing acute humanitarian needs and a civil war marked by consistently brutal tactics by the military regime.

The primary tool for arresting those who express dissent online is criminal charges under Sections 505 and 505-A of the Penal Code. Section 505-A, a new provision imposed by the military shortly after the coup, criminalises causing fear, spreading false news, or agitating for crimes against a government employee, and has been applied *en masse* to people who are affiliated with movements opposing the coup, as well as celebrities, artists, journalists, and those who post expressions of dissent on social media. In the year following the coup, almost 4,000 people were confirmed to have been arrested and detained under Sections 505 and 505-A, with the total number likely being much higher.[168] Other arrests have also been made under the Law on Counterterrorism and other older Myanmar criminal content restrictions.

Internet shutdowns and disruptions are now common in the country. Prior to the coup, Myanmar had already imposed one of the world's longest internet shutdowns, in the states

---

[165] International Crisis Group, *Myanmar's Military Struggles to Control the Virtual Battlefield*, 2021.

[166] Assistance Association for Political Prisoners, Daily Briefing in Relation to the Military Coup, 16 October 2023.

[167] International Commission of Jurists, Myanmar: A Year after Military Takeover, No Rule of Law or Judicial Independence, 10 February 2022.

[168] Free Expression Myanmar, *New Report: 505A Act of Revenge*, 31 January 2022.

of Rakhine and Chin, affecting over a million people.[169] Since the coup, internet shutdowns have become more common in other parts of the country as well. Access Now reports that in 2021 alone, the internet was disconnected 15 times in Myanmar, with the longest nationwide disruption lasting nearly 2.5 months.[170] These shutdowns have had devastating impacts, such as inhibiting essential supplies from reaching villages when drivers could not determine safe travel routes.[171] The military also appears to be using the shutdowns strategically, imposing disruptions prior to and during attacks on villages so as to avoid information about killings, torture, ill treatment, arrests, and arson – all of which are widespread – from being documented and shared.[172]

The military reliance on internet shutdowns may be partly a result of its limited technical capacity to block or intercept internet communications.[173] However, the military has also issued 'blacklists' to companies listing websites to be blocked, including major platforms like Facebook. It is apparently attempting to convert this into a 'whitelist' approach according to which only approved websites would be allowed.[174] These approaches may be replacing broader shutdowns in light of the military's lack of technical capacity to fully implement a controlled system similar to that of China or even Vietnam.

Pro-military media accounts have also engaged in online harassment and doxxing of activists and other people opposed to the military, sometimes accompanied by calls for violence or even the offering of rewards for their assassination. There is some evidence that these campaigns have been coordinated by or directly connected to military actors.[175] This context is very dangerous for journalists, activists, supporters of the political opposition, and indeed anyone expressing dissent. Military access to personal communications data can therefore be a life-or-death matter, as can platform policies regarding what posts are allowed.

Legal obligations on tech companies

Even before the coup, aspects of Myanmar's legal framework failed to protect freedom of expression and privacy, although Myanmar does not have such wide-ranging intermediary liability rules as China or Vietnam. The military's ability to enact laws is questionable under Myanmar's own constitution, given the fundamental illegitimacy of the military regime, but

---

[169] Human Rights Watch, Myanmar: End World's Longest Internet Shutdown, 19 June 2020.

[170] Access Now, *The Return of Digital Authoritarianism: Internet Shutdowns in 2021*, 2022.

[171] ARTICLE 19, Myanmar: Internet Shutdowns Shrouding Torchings and Killings, 23 June 2022.

[172] Access Now, *Weapons of Control, Shields of Impunity*, 2023.

[173] International Crisis Group, *Myanmar's Military*.

[174] Frontier Myanmar, Whitelisted Internet Takes Myanmar Back to a 'Dark Age', 30 June 2021; International Crisis Group, *Myanmar's Military*.

[175] A. Nachemson, 'Watermelon Suppression': Doxing Campaign Targets Pro-Democracy Soldiers and Police, Frontier Myanmar, 14 March 2022; OHCHR, Myanmar: Social Media Companies Must Stand Up to Junta's Online Terror Campaign, Say UN Experts, 13 March 2023.

the military has nonetheless imposed changes to Myanmar's legal regime which further complicate the environment for companies. The primary relevant laws include:

- Telecommunications Law 2013 (amended in 2017):[176] Several provisions of this law enable surveillance. Section 75 allows the government to require 'the relevant organisation' to provide access to information and telecommunications which cause harm to national security or respect for the law 'as may be necessary'. Although there is a clause calling for respect for fundamental rights, the vagueness of this provision and lack of concrete procedures could easily provide legal cover for problematic surveillance practices. Similar concerns are raised by Section 76, which enables entry and inspection of telecommunications service providers for matters related to national defence, security, or the public interest.

  In emergencies, Section 77 empowers the Ministry of Transport and Communications to order suspensions of telecommunications services, intercept or obtain information, cease operations of specific forms of communication, or temporarily control telecommunications equipment. 'Emergencies' are not clearly defined, and the military has declared the country under a state of emergency since the 2021 coup.

- Counter-Terrorism Act 2014 (amended in March 2023): Section 47 empowers a counter-terrorism committee to issue orders for the interception or restriction of electronic communications of 'terrorist groups and terrorists'.[177] The new Counter-Terrorism Rules issued in 2023 set out procedures for this interception. These rules lack basic due process protections, and the authorising committee is not independent from the military.[178] The rules explicitly state that telecommunications companies should not refuse the committee's orders to intercept or restrict communications.[179] These powers are likely to be applied extensively, as the military has applied the terrorist label broadly, including to members of the civil disobedience movement and peaceful opposition.

- Law Protecting the Privacy and Security of Citizens (2017; amended 2020 and 2021) (Privacy Law):[180] This law provides some very general privacy protections but does not constitute a proper data protection regime. Shortly after the 2021 coup, the military announced an amendment which suspended some sections of the law for as long as the

---

[176] Telecommunications Law, No. 31/2013, 8 October 2013, English translation; MLL Law Library, Pyidaungsu Hluttaw No. 26/17 : Amendment of Telecommunications Law, 28 August 2017, English translation. For a full analysis of this law see ARTICLE 19, *Myanmar: Telecommunications Law, 2013*, March 2017.

[177] Counter Terrorism Law, No. 23/2014, 4 June 2014, English translation.

[178] Access Now, Myanmar's 'Counter-Terrorism' By-Laws Must Be Denounced for What They Are – Illegal, 19 April 2023. For a partial English translation of the by-laws, see Lincoln Legal Services (Myanmar) Limited, Counter-Terrorism Rules, 1 March 2023.

[179] Lincoln Legal Services (Myanmar) Limited, Counter-Terrorism Rules, Rule 80(d).

[180] Law Protecting the Privacy and Security of Citizens, No. 5/2017, 8 March 2017, English translation (with post-coup military changes integrated).

State Administration Council governs the country.[181] The suspended privacy protections included prohibitions on telecommunications operators intercepting communications or accessing personal data without a warrant or lawful permission.

- The Electronic Transactions Law 2004 (amended in 2014 and 2021) (ETL):[182] The military introduced amendments to the ETL requiring those managing personal data to protect such information and imposing criminal penalties on those who obtain, disclose, use, destroy, or disseminate personal data without consent. These obligations are described only briefly and in very vague terms, posing serious compliance challenges for the private sector.[183] They also contain broad exceptions for government authorities, such as allowing it to gather information about cybersecurity issues of concern in relation to peace, stability, or national security, offering a legal excuse for the government access to personal data.

- Draft Cybersecurity Law (2021; 2022): The military circulated a draft Cybersecurity Law just days after the 2021 coup. IT dropped this draft after substantial backlash from the business community and civil society, although a few provisions were integrated into subsequent amendments to the ETL.[184] In 2022, a revised draft was proposed.[185] It is unclear whether the military still intends to introduce this law, which raises serious freedom of expression and privacy concerns. The draft law would impose registration requirements and other onerous obligations on digital service providers, create new intrusive regulatory powers over such providers, and impose local data storage requirements. It would also criminalise the use of VPNs without government permission.

Myanmar law enables surveillance and lacks a proper personal data protection regime. It empowers authorities to interfere with internet services and order restrictions on information. Particularly in the current context, where Myanmar's military has issued martial law orders and claims an ongoing emergency, this legal framework enables extensive violations of the rights to freedom of expression and privacy. With the collapse of the rule of law in post-coup Myanmar, military *de facto* actions may be more important than the letter of the law, but the

---

[181] Myanmar News Agency, Amendment of Law Protecting the Privacy and Security of the Citizens, 13 February 2021, English translation, 14 February 2021.

[182] Electronic Transactions Law (Consolidated Version) based on State Peace and Development Council Law No. 5/2004, 30 April 2004, English translation incorporating 2014 amendments and 2021 post-coup changes.

[183] Allen & Overy, *Update from On the Ground: Changes to the Electronic Transactions Law and the Impact on Financial Institutions operating in Myanmar*, 15 March 2021, 2.

[184] See description of developments at Myanmar Centre for Responsible Business, Update on Draft Cybersecurity Law and its Impacts on Digital Rights and the Digital Economy, 15 February 2022; ARTICLE 19, Myanmar: Scrap Cyber Security Draft Law and Restore Full Internet Connectivity, 12 February 2021.

[185] Free Expression Myanmar, Cyber Security Law (Draft), State Administration Council Law No.-/2022, English translation with annotated changes from the earlier draft. For analysis and commentary on this draft, see Centre for Law and Democracy, Myanmar: Note on New Draft Cyber Security Law, April 2022; Access Now, Analysis: The Myanmar Junta's Cybersecurity Law Would Be a Disaster for Human Rights, 27 January 2022; Free Expression Myanmar, Military's Cyber Security Bill Worse Than Their Previous Draft, 27 January 2022.

legal framework also empowers the military to demand that private companies cooperate with its human rights violations.

Tech company responses

Since the February 2021 coup, Myanmar's military has been unable to fully enforce its desired control of the online information space. This is partly because prominent platforms have not recognised the military as the legitimate government and, in an unusual move, have deplatformed or removed content from military-linked accounts. The first case study below offers a closer look at these actions. These companies also appear to be refusing to cooperate with military requests. After the coup, Facebook explicitly said that it had 'indefinitely suspended the ability for Myanmar government agencies to send content removal requests to Facebook through our normal channels reserved for authorities around the world'.[186]

The non-compliance has had 2 notable consequences. First, the military's main option vis-à-vis tech companies is to block them altogether. Since the days immediately following the coup, it has issued blocking orders for Facebook, WhatsApp, Twitter, and Instagram. Such blocking orders have not always been very effective, though, since service providers have implemented them inconsistently and because many users use VPNs to get around them.[187] The military has certainly restricted access to such services, but it has not managed to completely prevent their use.

Second, the deplatforming of the military on key platforms and military attempts to restrict access to such apps have splintered and changed the digital market, with Myanmar users relying on a much broader array of applications than previously.[188] From a corporate responsibility perspective, this means that the actions of one company are less significant. Before the coup, attention had been focused on Facebook's failures in Myanmar. Now, industry-wide action is needed, but as highlighted in the case study below, company reactions have been mixed.

Although the military has struggled to control content on foreign tech platforms, it has effectively taken control of telecommunications service providers and much of the country's internet infrastructure, enabling it to order internet shutdowns or blocks as well as the sharing of user data or the installation of surveillance tools. Myanmar has 4 telecommunications service providers, 2 of which were already linked to the military before the coup. Mytel, for example, is a joint venture of the Myanmar and Vietnamese militaries and is particularly distrusted by those opposed to the military, with armed resistance groups

---

[186] R. Frankel, An Update on the Situation in Myanmar, Meta, 11 February 2021.

[187] International Crisis Group, *Myanmar's Military*.

[188] H.O. Faxon, K. Kintzi, V. Tran, K.Z. Wine, and S.Y. Htut, Organic Online Politics: Farmers, Facebook, and Myanmar's Military Coup, *Big Data and Society*, 16 April 2023.

having destroyed some of its towers since the coup.[189] The 2 foreign firms in the country were the Norwegian company Telenor and the Qatari-owned Ooredoo. Telenor has now sold its Myanmar operations to a military-linked company, as described in the case study below; Ooredoo is seeking Myanmar military approval for a similar sale. Both companies had been under pressure from the military, which had ordered them to install surveillance software in the months before the coup.[190]

The main check on the military's ability to restrict internet content and conduct surveillance is likely technical capacity limitations. While the military's technical capacity is generally perceived to be relatively poor, at least in comparison with that of China and Vietnam, activists have said that they cannot take this for granted, given the high stakes involved and because the military uses an array of tactics to track people beyond simply issuing orders to telecommunications companies.[191]

The military is actively working to expand its access to surveillance technology, including through purchases from foreign companies, although this is secretive and public information on such transactions is not readily available. Chinese firms have provided CCTV and biometric technology to Myanmar on an ongoing basis, for example.[192] Indian firm Bharat Electronics, primarily owned by the Indian Government but with other shareholders including Goldman Sachs, has also provided military and dual-use technology to the military.[193] Lack of transparency surrounding deals made before the coup makes it challenging to assess what surveillance tools the military has at its disposal. For example, Israeli company Cognyte Software won a contract to sell intercept spyware to Myanmar a month before the coup.[194]

A full discussion of issues regarding the trade in surveillance technology and spyware is beyond the scope of this paper.

---

[189] Reuters, Attacks on Myanmar Telecom Towers Show Evolving Tactics in Conflict, 17 September 2021.

[190] F. Potkin and P. McPherson, How Myanmar's Military Moved in on the Telecoms Sector to Spy on Citizens, Reuters, 18 March 2021.

[191] Interview with Golda Benjamin, Access Now.

[192] Access Now, Track and Target: FAQ on Myanmar CCTV Cameras and Facial Recognition, 4 August 2022; ARTICLE 19, Who Buys and Controls the CCTV? Myanmar's Slippery Slope to Mass Surveillance, 2022.

[193] Justice for Myanmar, Bharat Electronics Limited Supplying Technology to Myanmar since Attempted Military Coup, 14 June 2021.

[194] F. Potkin and P. Mcpherson, Israel's Cognyte Won Tender to Sell Intercept Spyware to Myanmar before Coup – Documents, Reuters, 18 January 2023.

Myanmar provides an important example of why discussions about the roles of foreign tech companies must also cover surveillance and spyware companies, as these industries operate secretively and are much harder to influence via public pressure campaigns.

However, Myanmar watchdog groups have actively tried to pressure them.[195]

Case study: Platform reactions to military content after the 2021 coup

Several tech companies announced measures to remove military content from their platforms following the 2021 coup. Shortly after the coup, Meta announced that it would reduce the distribution of content from military-run channels which shared disinformation. Then, on 24 February 2021, it banned all military and military-controlled accounts from Facebook and Instagram, along with ads from military-linked businesses. It cited the military's history of severe human rights abuses and repeated violations of platform policies, as well as ongoing violations, the risk of future violence, and the increased risk since the coup that online threats would lead to offline harm.[196] Several weeks later, Meta announced a specific policy on removing posts which praised or supported violence by Myanmar security forces against protesters, and in December 2021, it banned military-linked businesses from the platform.[197]

With the military losing easy access to Facebook, it tried moving to other platforms, including YouTube, VK, and TikTok. Following Meta's lead, YouTube removed 5 of the military-run television networks in early March 2021. However, it has not publicly announced Myanmar-specific actions since then, and digital rights activists suggest that it has done little in practice.[198]

TikTok was slower to respond initially and was subject to criticism for hosting military propaganda, including of soldiers making violent threats and brandishing weapons.[199] The Myanmar ICT for Development Organisation (MIDO) documented more than 800 pro-military videos threatening protesters as of early March 2021.[200] In response to this study and other public criticism, TikTok acknowledged that it had been slow to act but claimed it

[195] See, for example, Justice for Myanmar, Tools of Digital Repression, 2 March 2021; Burma Campaign UK, The Dirty List, August 2023.
[196] R. Frankel, An Update.
[197] R. Frankel, An Update.
[198] Freedom House, Freedom on the Net 2023: Myanmar (citing discussions with digital rights defenders).
[199] International Crisis Group, *Myanmar's Military*, p. 22.
[200] Reuters, 'I Will Shoot Whoever I See': Myanmar Soldiers Use TikTok to Threaten Protesters, 4 March 2021.

had since 'aggressively banned' numerous accounts.[201] It also took steps such as issuing new guidance to its moderators and expanding partnerships with Burmese civil society.[202] However, TikTok has also faced ongoing challenges regarding content moderation in Myanmar, partly because the military's behaviour on the platform is different from its behaviour on other platforms, with soldiers less likely to wear uniforms and show weapons, demonstrating the need for the company to scale its content moderation efforts.[203]

X (formerly Twitter) has also become more popular in Myanmar since the coup and, although it appears more popular with activists than the military, there have been issues with the company failing to take action against military-affiliated misinformation.[204] Since Elon Musk's takeover of the platform in 2022, some Myanmar activists who use X have voiced concerns about a decline in content moderation enabling the proliferation of military accounts and about Musk's threat to require user authentication compromising the anonymity and security of at-risk activists.[205] The extent to which these fears are justified depends somewhat on future policy choices at X, although a decline in content moderation at X has been observed globally.

Google has also taken some actions to remove military content, taking down a military propaganda blog from its Blogger platform and reviewing advertisements run by Mytel, in both cases after activists campaigned for them to remove the content.[206] Both the Google and the Apple app stores also removed an app developed by the Myanmar military for its military-controlled broadcaster in 2022, a day after its launch, after campaigners called for its removal.[207] Google and Apple have, however, failed to remove other military-associated apps, as called for by advocates, such as the military's OKPar, which is supposed to be a Facebook alternative.[208]

Many major tech companies have, therefore, taken at least some action against military content on their platforms. A notable exception is Telegram, where the military has found a safe haven as other platforms have become more inaccessible. UN experts have warned that Telegram has become a 'hotbed' of pro-military activity, including violent and

---

[201] K. Lyons, TikTok Banning Some Accounts in Myanmar, 20 March 2021.

[202] International Crisis Group, *Myanmar's Military*, p. 22.

[203] International Crisis Group, *Myanmar's Military*.

[204] E. Hale, From China to Thailand, Dissidents Fear Musk's Twitter Reign, Al-Jazeera, 7 November 2022.

[205] Hale, From China to Thailand; A. Deck, E. Fishbein, and G. Glatsky, Where Anonymity on Twitter Is a Matter of Life or Death, *Rest of World*, 6 May 2022.

[206] J. Elder, Google Has Pulled Down a Propaganda Blog Backing the Military Coup in Myanmar after Outcry by Online Activists, Business Insider, 20 February 2021; F. Potkin, Google and Viber Review Adverts for Myanmar Military Backed-Telecoms Firm, *Reuters*, 10 March 2021.

[207] Justice for Myanmar, US Tech Firms Enabling Myanmar Junta Propaganda, 5 May 2022; The Irrawaddy, Myanmar Junta Propaganda App Ditched by Apple and Google, 7 May 2022.

[208] Access Now, Meta and Google Must Use Their Powers to Stop Myanmar's Alternative Propaganda Machine, 21 September 2021 (OKPar was also still available on both app stores at the time of writing).

misogynistic content.[209] Pro-military accounts on the platform have spread military disinformation and propaganda and doxxed opponents of the coup, posting their personal information along with violent threats, calls for their arrest, and screenshots of their social media accounts, or posting sexually explicit (often fabricated) images of female activists.[210] Telegram, which is famous for its 'light-touch content moderation',[211] has engaged in little moderation of such content. In response to public pressure, it removed several pro-military channels for violating its terms of service in March 2023, but many other pro-military channels have remained on the platform and there are ongoing problems with doxxing.[212]

Overall, military content, including misinformation, hate speech, and violent threats, remains a recurrent problem across online platforms, particularly on Telegram. A Reuters story in November 2021, for example, said that it had identified about 200 military personnel posting misinformation on Facebook, YouTube, Twitter, and Telegram, with content often duplicated across dozens of copycat accounts within minutes.[213]

One reason for this is that while companies have announced actions which appear to be notable, taking consistent action to remove problematic content is more challenging. For example, Facebook has perhaps been the most active in responding, likely because it has been more engaged in content moderation in Myanmar since it became infamous as a vehicle for hate speech against the Rohingya in 2018. Its actions have had a real impact, forcing military accounts to relocate to Telegram. However, military-related accounts and speech which violates Meta's policies are still regularly identified on Facebook, and one civil society organisation has noted that its algorithm appears to be continuing to promote such content when it is not removed.[214]

Myanmar digital rights activists have been organised in highlighting harmful content and tagging it for platforms, for example by coordinating to report when the military creates new Facebook pages.[215] A key challenge for civil society and advocates in Myanmar has been been getting platforms not only to respond but to respond quickly enough, as military actors

---

[209] OHCHR, Social Media Companies Must Stand Up to Junta's Online Terror Campaign.

[210] A. Nachemson, Channelling Hate and Disinformation: Myanmar's Bad Actors Move to Telegram, *Frontier Myanmar*, 15 September 2021; BNI, How Myanmar Lobbyists Use Telegram to Spread Propaganda, Fake News, 9 June 2022; Mi-Kun, In Myanmar, Telegram Is Used as a Weapon to Destroy Lives, EngageMedia, 26 July 2023.

[211] C. Crystal, Facebook, Telegram, and the Struggle against Online Hate Speech, Carnegie Endowment for Peace, 7 September 2023.

[212] Nang, Despite Takedowns, Pro-Military Doxing Rampant in Myanmar Telegram Channels, Rappler, 22 August 2023.

[213] F. Potkin and W. Lone, 'Information Combat': Inside the Fight for Myanmar's Soul, Reuters, 2 November 2021.

[214] Global Witness, Algorithm of Harm: Facebook Amplified Myanmar Military Propaganda Following Coup, 23 June 2021 (note, however, that this conclusion appears to be based on a single test); Associated Press, Hate Speech in Myanmar Continues to Thrive on Facebook, NBC News, 18 November 2021.

[215] International Crisis Group, *Myanmar's Military*, p. 21.

have multiple accounts on different platforms and can easily jump platforms or change accounts on the same platform, taking their followers with them.[216] Telegram links are posted on TikTok and Facebook accounts to maximise their reach, for example, allowing problematic content to jump platforms.[217] Users have also taken to posting subtler content which is harder for platforms to detect.[218] Platforms need to make sustained investments in content moderation in response, including using moderators who have knowledge of the local context.

Case study: Telenor in Myanmar

Telenor is a telecommunications company majority-owned by the Norwegian state. In 2013, it won a competitive bid for one of 2 nationwide telecommunication licences offered by the Government of Myanmar.[219] Its wholly owned subsidiary, Telenor Myanmar, introduced a mobile phone network across the country in 2014. By 2020, Telenor Myanmar had over 18 million mobile subscriptions, covering 92% of the population.[220] It was a favoured choice of activists and human rights defenders because it was perceived as being safer and more rights-protective than the military-owned alternatives or Qatar's Ooredoo.

After the coup, Telenor and other telecommunications operators started to receive daily notices to blacklist certain websites and VPNs, and they also came under pressure to share user information with the military.[221] This put Telenor in a difficult human rights position, although the pre-coup government had also asked Telenor to cooperate in internet shutdowns in the states of Rakhine and Chin, so this was not an entirely unprecedented problem. Before the coup, Telenor had said it was in 'continuous dialogue' with authorities to restore access, while following the coup such dialogue was likely implausible.[222]

In any case, Telenor decided it could no longer sustain operations in the country. Its statements in relation to the decision cited 'our own values on human rights and responsible business' and conflicts between Myanmar and European laws, as well as the safety of its employees.[223] In July 2021, it announced the sale of its Myanmar subsidiary to M1 Group, a Lebanese firm. The military initially blocked the sale, likely because it wanted to ensure that a local military-affiliated company was involved. The sale was eventually finalised in March 2021, after the Myanmar military approved an arrangement by which M1 granted a majority stake to Shwe Byain Phyu, a Myanmar entity with military ties.[224]

---

[216] Interview with Dhevy Sivaprakasam, Access Now.

[217] Mi-Kun, In Myanmar.

[218] International Crisis Group, *Myanmar's Military*.

[219] Mizzima, Telenor Promises State-of-the-Art Network, BNI, 28 June 2013.

[220] Telenor, Building a Network, Connecting a Nation.

[221] Mi-Kun, In Post-Coup Myanmar, Telco Operators Act as the Military's Eyes and Ears, EngageMedia, 31 July 2023.

[222] Telenor, Continued Network Restrictions in Myanmar from 1 August 2020 (Updated 31 December 2020.

[223] Telenor, Sale of Telenor Myanmar Approved by Myanmar Authorities, 18 March 2022.

[224] P. McPherson and F. Potkin, Myanmar Firm Poised to Control Telenor Unit after Military Backs Bid, Reuters, 11 February 2022.

Telenor's sale was controversial for a number of reasons. First, M1 Group itself has a reputation for working with authoritarian regimes while disregarding human rights, including operating mobile networks in Yemen, Syria, Liberia, and Sudan, the last of these including during the Darfur genocide.[225] Second, the inclusion of Shwe Byain Phyu gave the military direct access to the successor company. Third, there was significant concern that the sale would involve the transfer of sensitive personal data which could then be accessed by the military, as well as technology which could potentially be misused by the military to target human rights defenders and activists.

Civil society and advocacy organisations campaigned extensively around the Telenor sale, hoping to mitigate its harms if it was not possible to block it completely. This included a challenge by 474 Myanmar civil society groups represented by the Dutch NGO SOMO (the Centre for Research on Multinational Corporations) at the OECD's Norwegian National Contact Point – a mechanism which allows complaints against companies based in countries which have committed to the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. The complaint argued that Telenor had not conducted appropriate due diligence, had not sufficiently engaged relevant stakeholders in relation to the sale, and had not been transparent about its decision to exit Myanmar.[226] While the complaint was not successful at stopping the sale, following mediation SOMO and Telenor signed a Memorandum of Understanding in which Telenor agreed to conduct an internal review process, fund an independent study, and explore the creation of a 'digital security relief mechanism' to provide financial, legal, and training support to Myanmar citizens facing risks associated with their exit from the country.[227]

Telenor did engage somewhat with civil society, but it argued that it could not comply with many of their demands due to its obligation to protect the safety of its in-country employees. For example, when human rights groups pressured Telenor to ensure that its data was not handed over to the military, Telenor said that closing operations and deleting data would have placed employees in Myanmar 'at considerable risk'.[228] Telenor certainly was in an extremely challenging situation, especially in relation to some of its employees, who were prevented from leaving the country. However, it could have done much more, including conducting better human rights due diligence when it entered the market in the first place, being much more transparent about its actions, and doing more to reach out to impacted groups following the coup. It is also not clear whether Telenor rigorously mapped the potential rights impacts of its sale and incorporated such mapping into its decision-making.

---

[225] Justice for Myanmar, Exposing the Business Networks Fuelling Brutality and Corruption, 9 July 2021.
[226] OECD Watch, SOMO Representing 474 Myanmar CSOs vs. Telenor ASA, 27 July 2021.
[227] OECD Watch, SOMO Representing 474 Myanmar CSOs vs. Telenor ASA.
[228] Telenor, Updates from Telenor Group on Developments in Myanmar Since 1 February 2021.

Tech company responses and the UN Guiding Principles

This review of tech company responses to digital authoritarianism in China, Vietnam, and Myanmar reveals some common threads. We highlight 5 key issues below.

Deferring to local laws when explaining actions in violation of human rights

First, tech companies more or less consistently defer to local law and rely on this justification when explaining their decisions to take actions which compromise human rights. Such deference to local law is consistent across the companies that have remained active in the focus countries and across countries. Although some companies made general references to the UNGPs or human rights, none provided detailed information about how they resolve conflicts between local law and human rights responsibilities. Instead, they appear to have accepted local legal regimes largely at face value.

The UNGPs acknowledge that companies must abide by local law, but they also indicate that where domestic law and human rights principles conflict, businesses should respect human rights principles 'to the greatest extent possible in the circumstances', and that they should be able to demonstrate their efforts to do so. This means that they cannot merely defer to the need to follow local law.

As highlighted already:

---

the GNI provides concrete guidance on navigating such situations, including demanding specificity and clarity from governments, requiring governments to show the legal basis for requests, and interpreting government demands narrowly. It also encourages companies to take steps such as seeking modifications to such demands or challenging them in local courts.

Unfortunately, the situations highlighted in this report do not provide much evidence that companies are respecting the UNGPs or the GNI principles in practice. For example, the UN Special Rapporteur on freedom of expression, in a letter to Apple, asked for clarification about its decision to remove VPN apps from its app store, which it had said it did to meet new regulations. The Special Rapporteur asked for more information about whether Chinese authorities had specifically requested the removal of these apps, the legal analysis Apple relied on to determine that it was required to remove the apps, whether it considered China's human rights obligations in its analysis, whether it objected to the application of Chinese law or raised non-legal concerns with authorities, and what processes it had for making the

decision.[229] Making this kind of information public would have greatly clarified the extent to which Apple was actually incorporating the UNGPs into its decision-making process. Apple failed to respond, indicating that it was not prepared to demonstrate its efforts to ensure respect for human rights, and certainly not 'to the greatest extent possible in the circumstances', as called for in the UNGPs.

Similarly, in the specific context of government requests for content removal, companies should not blindly accept local authorities' arguments that content is illegal, particularly where the takedown is not ordered by a court or independent entity. However, in Vietnam, for example, companies appear to have acted on government takedown requests even when the requests were based on broadly worded content restrictions which clearly conflict with human rights law, such as 'opposing the Communist Party and the Government of Vietnam'. In other cases, tech company transparency reports do not mention the legal bases for the requests or describe them only in very general terms. Tech companies should provide much more detailed information about the legal bases for government requests and whether and how they push back on such requests.

Admittedly, this report focuses on highly authoritarian contexts where companies have been exposed to retaliation if they are deemed not to have complied sufficiently with government censorship demands, such as the throttling of Facebook in Vietnam. In other countries in the region, there are examples of tech companies objecting more strenuously to government demands, such as in India, where Twitter and WhatsApp tried to bring lawsuits, respectively challenging takedown orders and a requirement to stop offering encryption.[230] However, problems of insufficient transparency and an apparent lack of policies and practices on challenging government demands appear to be systemic and can be observed in tech company operations around the region (and globally).

Lack of transparency

Second, a lack of transparency is a major problem with the tech companies discussed in this report. UNGP 21 says that businesses for which operations or operating contexts pose risks of severe human rights impacts should report formally on how they address these risks, in a qualitative, systematic, and regular form and providing enough information that the adequacy of their responses can be evaluated.

Although more tech companies are now adopting 'transparency reports', these typically offer minimal country-specific information and report in such a general manner that they provide little guidance on the extent to which tech companies are identifying human rights risks in

[229] UN Special Rapporteur, Letter to Tim Cook.

[230] H. Ellis-Petersen, WhatsApp Sues Indian Government over 'Mass Surveillance' Internet Laws, *Guardian*, 26 May 2021; M. Vengattil, Twitter Seeks Judicial Review of Indian Orders to Take Down Content, Reuters, 6 July 2022.

authoritarian contexts and adopting risk management strategies in response. Some companies have provided next to no information about particular human rights controversies. Bing has disclosed very little information about how it responds to Chinese censorship demands, for example. In Myanmar, beyond initial public announcements about actions taken to ban military accounts, most companies have not released detailed updates about how they are responding to ongoing military-inspired harmful speech on their platforms.

Lack of country-specific human rights due diligence

Third, tech companies should engage in regular, country-specific human rights due diligence. The case studies in this report show that there is little evidence that such due diligence is being undertaken. As outlined in the UNGPs, this should be an ongoing exercise with multiple steps, including identifying and assessing impacts, acting to prevent and mitigate risks, tracking the effectiveness of risk mitigation, and appropriate communication of performance.[231]

Most tech companies covered in this report do not appear to be engaged in ongoing human rights due diligence specific to China, Vietnam, or Myanmar, or at least they do not publicise it. Even where companies have engaged in due diligence, it has not been sufficiently comprehensive and ongoing. Telenor commissioned a human rights impact assessment before it entered Myanmar in 2014 but seemingly failed to maintain adequate ongoing assessments, including advanced planning for a responsible exit.[232] An example of a flawed approach to human rights impact assessments in the region is given in the box below. Overall, tech companies operating in authoritarian countries in Asia need to devote much more leadership, planning, and resources to human rights due diligence.

[231] B-Tech, Taking Action to Address Human Rights: Risks Related to End-Use, OHCHR, September 2020, p. 2 (providing a graphical summary).

[232] Telenor, Human Rights in Myanmar. Telenor Myanmar did release annual 'sustainability briefings'.

Example: Meta's human rights impact assessments in Asia

As part of its response to its failures in Myanmar, Meta commissioned an independent organisation to conduct a human rights impact assessment of its operations there. It subsequently made this assessment public along with its response. Since then, it has commissioned other national human rights impact assessments, publishing reports for Cambodia, the Philippines, Indonesia, and Sri Lanka.[233]

Human rights impact assessments are a crucial part of the due diligence called for in the UNGPs. It is best practice for tech companies to conduct such assessments regularly and to release them publicly. Unfortunately, however, Meta's responses have been sporadic and reactive, rather than resulting from a proactive policy of running such assessments regularly in high-risk contexts as a preventative measure. Most notably, Meta declined to disclose its full impact assessment for India, which was commissioned in 2019. This is controversial and not in accordance with the UNGPs. The assessment was meant to be an independent evaluation of Meta's role in the spread of hate speech and incitement to violence in India.[234] Meta cited security concerns as a reason for not releasing the report,[235] but if any part of the report posed a genuine threat to someone, that portion could easily have been redacted.

Lack of sector-wide mobilisation and industry standards

As shown by the case studies in this report, the fragmentation of the online space has complicated human rights impacts. A diversity of services is an overall positive for freedom of expression online, and the monopolistic behaviour of many tech companies should be condemned. However, addressing harmful speech across platforms is also a real challenge, as evidenced in Myanmar, where the military has responded to bans by rapidly creating new accounts and jumping platforms. The existence of 'bad actors' like Telegram, which has refused to engage seriously with harmful speech on its platform, highlights that action by one or a few companies is not enough. Similarly, in China, local companies which do not make human rights commitments can fill the gap left by exiting Western companies.

[233] Meta, Our Impact: Meta Human Rights Impact Assessments.

[234] D. Brown and J. Bajoria, Meta and Hate Speech in India, Human Rights Watch, 21 July 2022.

[235] ARTICLE 19, Meta: Transparency Vital for Protecting Human Rights in India and Palestine, 25 August 2022.

There is no easy answer to this problem. Nonetheless:

The tech sector needs to consider how it can mobilise greater sector-wide action and develop stronger industry standards on human rights. Where the choice is between exiting a country and complying with human rights violations, tech companies should engage in transparent, responsible exit discussions, including clearly and publicly accounting for how they make decisions to stay or leave based on human rights, legal, and commercial considerations. Tech companies should not rely on general references to the importance of staying in a particular market to explain compliance with government demands, as Facebook has sometimes done in Vietnam.

This report offers some practical lessons about how tech companies can be most successful in promoting human rights in authoritarian contexts. Tech companies have had some success when presenting organised opposition to data localisation requirements. Industry voices seemed to have an impact on the military in Myanmar withdrawing the draft Cybersecurity Law and on the easing of a data localisation requirement in a proposed Vietnamese regulation. One reason for this is that companies can make a strong economic and commercial case for the harms of data localisation – an argument that authoritarian regimes may be more responsive to. However, tech companies should also speak out more frequently, and collectively, on other issues which raise freedom of expression and privacy concerns.

Devoting resources and staff to human rights issues also matters. In Myanmar, Facebook's past scandals meant that it had developed Myanmar-specific knowledge and staff, and it was relatively better equipped than other companies to respond to the 2021 military coup, although the consistency of its response has been a concern. In contrast, the consequences of inadequate human rights staffing by Facebook in Vietnam, or at least insufficient outreach by this staff to local civil society groups, has meant that it has failed to develop a strong strategy for misuse of its content moderation system by government-linked users.

Lack of comprehensive partnership with civil society

Finally, this report also highlights the crucial role of civil society. Tech companies are often slow to act until they receive negative publicity. In Myanmar, companies have often removed content because of campaigning by civil society, including eventually even Telegram. In Vietnam, civil society has had to take the lead in reaching out to Facebook to combat abuse

of its complaints system. In China, although the space for domestic civil society is very constrained, international advocates have helped to draw attention to tech company cooperation in Chinese censorship, such as by flagging and tracking content removals. Local civil society often has good knowledge of the local context and may be aware of security risks facing local human rights defenders. Companies can benefit from partnerships with these groups, although they need to be cautious of overburdening non-profits with requests for assistance, given that such groups typically operate with constrained resources and budgets, and of creating risks for them.

Tech companies have human rights responsibilities, even when operating in highly authoritarian contexts. Although tech companies reference the UNGPs, they generally do so only in a superficial manner or read the UNGPs as allowing them to cite local law as a justification for cooperating in human rights abuses.

Tech companies should integrate the UNGPs into their operations in a much more rigorous manner, putting in place transparent systems for handling problematic government requests, reporting transparently on how they respond to these requests, and pushing back on requests based on vague or unclear laws.

They should also explore broader industry-wide advocacy for a range of freedom of expression and privacy issues and not merely those that carry a heavy commercial burden (such as data localisation requirements). In an era of tech sector lay-offs, companies should continue to allocate sufficient resources and staffing to human rights issues.

So far, tech company leadership in implementing the UNGPs in authoritarian countries in Asia has been lacking.

Recommendations

Recommendations for governments in the region

Governments in the region should:

- revise their legal frameworks to bring them into line with international human rights standards, including on freedom of expression and privacy;
- recognise their responsibilities under the first pillar of the UN Guiding Principles (UNGPs) and human rights law, and avoid compelling or pressuring companies to breach their human rights responsibilities;
- foster universal access to an open internet, avoiding shutdowns and unnecessary restrictions on online platforms, and facilitating a vibrant online ecosystem; and
- protect human rights defenders and activists, including by taking measures to prevent harassment, threats, or violence against them and immediately and unconditionally releasing individuals who have been wrongly detained or imprisoned solely for exercising their right to freedom of expression and other human rights.

Recommendations for tech companies operating in authoritarian contexts

Tech companies operating in authoritarian contexts should:

- uphold human rights standards in accordance with the UNGPs;
- conduct human rights due diligence, including by undertaking regular human rights impact assessments; these should be country specific and disclosed publicly, the process should be transparent and should involve meaningful consultation with affected stakeholders, and once assessments are completed, effective measures should be put in place to mitigate identified risks;
- develop, publish, and fairly apply clear policies and procedures for content moderation, including specific standards for responding to government requests to remove content, and ensure that they reflect the principles articulated in the Santa Clara Principles;
- develop clear policies on how they will respond to government requests to restrict services or share user data that include reasonable efforts to resist such requests, such as a commitment to evaluate each request individually and challenge the legality of requests as appropriate;
- prioritise transparency and accountability: transparency reports should be more regular and more detailed than is currently standard practice and should include country-specific commentary on steps taken to comply with and challenge local law, as well as more detail on content which has been removed at the request of both governments and users; companies should also be transparent about how they negotiate and the conditions for

their market access, as well as any licences, contracts, or permissions they receive from the government;

- provide tools for user privacy and security: implement privacy by design and empower users to control their personal data;
- ensure appropriate support for their local country teams, including rapid responses and assistance when human rights concerns are raised by local or regional staff;
- support freedom of expression initiatives in the Asia region, such as through providing financial support and technical expertise and collaborating with civil society and other human rights defenders; and
- engage in multi-stakeholder and industry-wide dialogue and pursue initiatives designed to enhance industry-wide collaboration on human rights issues.

Recommendations for tech companies operating in China

Tech companies operating in China should:

- provide clear public reporting on the extent to which Chinese authorities have demanded access to user data, the types of data these authorities have been granted access to, and the circumstances surrounding such access, as well as taking other steps to enhance the privacy protection of user data and resist data localisation (or, if this is impossible, to transparently report on data localisation and associated risks for users);
- publicly report on actions taken to alter their existing moderation systems or algorithms in response to legal requirements;
- pursue legal mechanisms for challenging censorship orders and avoid taking censorship actions before exhausting other alternatives, while ensuring transparent reporting on all such actions and government demands; where they do ultimately restrict content within China, screen for any impacts of such content restrictions on access to that content outside China, and adopt tailored policies and technical solutions in response; and
- conduct more exhaustive due diligence, in line with the UNGPs, across their Chinese operations, and incorporate human rights considerations into decisions on whether they enter or exit China.

Recommendations for tech companies operating in Vietnam

Tech companies operating in Vietnam should:

- establish communications channels with local Vietnamese civil society organisations to help human rights defenders access support from the company when they are targeted online;

- develop strategies for responding to coordinated abuse of content moderation systems, including Vietnam-specific responses;
- expand and collaborate with industry-wide advocacy efforts, including to ensure that they are informed by an evaluation of human rights concerns and risks for users;
- report transparently on possible government surveillance via their platforms and on any actions which would enable government access to user data in Vietnam, including government requests for such data;
- regularly reassess their bargaining power and ability to challenge government demands for cooperation in human rights violations, and tailor their actions accordingly;
- cooperate with both domestic and international researchers to enable better reporting on government operations such as Force 47 and civilian counterparts; and
- recognise that local companies are under intense pressure to cooperate in human rights violations, and integrate this knowledge into their human rights due diligence and risk mitigation measures when working with local businesses.

Recommendations for tech companies operating in Myanmar

Tech companies operating in Myanmar should:

- adopt Myanmar-specific human rights strategies and policies that are conflict-sensitive, responsive to the reality of a multilingual and multi-ethnic society, and reflect the real dangers faced by users of retaliation based on their use of online platforms;
- consider a multi-company mechanism to promote coordination among the main tech platforms operating in Myanmar, including the possibility of taking rapid action in response to highly harmful content;
- establish ties with civil society and exile groups which can provide necessary context and information regarding the local impact of their policies and operations;
- allocate appropriate staff and resources to Myanmar-focused human rights operations, including staff with local knowledge and languages;
- report regularly on actions taken to implement Myanmar-specific policies announced after the 2021 coup, as well as earlier policies such as those responding to anti-Rohingya hate speech, and regularly revise and update these policies; and
- report publicly on the risk of military access to user data and establish systems for communicating these risks to local groups.


ARTICLE 19