CENTER FOR DEMOCRACY & TECHNOLOGY

The Promise and Challenge of Strategic Trade Engagement in the Indo-Pacific Region

Before the U.S. Senate Committee on Finance

March 15, 2022

Testimony of Emma Llansó, Director, Free Expression Project
Center for Democracy & Technology

Chairman Wyden, Ranking Member Crapo, and Members of the Committee,

Thank you for the opportunity to testify before you today about the opportunities for advancing digital rights and fostering robust digital economies through strategic trade engagements in the Indo-Pacific region. My name is Emma Llansó and I am the Director of the Free Expression Project at the Center for Democracy & Technology (CDT), where I have worked for more than twelve years to promote law and policy that support Internet users' rights to freedom of expression, access to information, and privacy in the US, Europe, and around the world.

CDT is a nonpartisan nonprofit 501(c)(3) charitable organization dedicated to advancing civil rights and civil liberties in the digital world. Headquartered since 1994 in Washington, DC, and with a growing office in Brussels, Belgium, CDT works to ensure that human rights and civil liberties are at the forefront of policy debates around the Internet and emerging technologies, and to advance policy solutions that sustain an open, interconnected Internet that supports people's enjoyment of their human rights.

So I am grateful for the Committee's focus on the promises and challenges in the digital sphere that will arise as the United States pursues closer trade relations in the Indo-Pacific. Over half of the world's young population lives in the Indo-Pacific region, which makes up 60% of the global GDP and nearly two-thirds of global economic growth.[1] It accounts for a little over half of the world's Internet users,[2] and Internet use in the Indo-Pacific Region is expected to grow to up to 3.1 billion users by 2023.[3]

There is an urgent need to counter the authoritarian model of Internet regulation promoted by the Chinese government, which threatens human rights and impedes the development of an open digital economy. Indeed, there are an alarming number of recent laws and legislative proposals across the

---

[1] White House, *Indo-Pacific Strategy of the United States* 4-5 (Feb. 2022) [https://perma.cc/7PSM-QDY2].
[2] Trisha Ray et al., *The Digital Indo-Pacific: Regional Connectivity and Resilience*, QuadTech Network at 1 (Feb. 2021) [https://perma.cc/BPL6-9WW6].
[3] Cisco, *Annual Internet Report* 3 (2020) [https://perma.cc/9TJA-MJ6Z].

Indo-Pacific region that seek to control speech and access to information, subject Internet users to surveillance, and give state authorities control over Internet infrastructure.

The US has the opportunity, including through the Indo-Pacific Economic Framework (IPEF) discussions, to promote a rights-respecting, multistakeholder approach to Internet governance that ensures the participation of civil society and technical experts in the development of technology policy and prioritizes maintaining an open, interconnected Internet in the region and worldwide. It should promote the rule of law and seek commitments to uphold international human rights, which are vital to countering digital censorship and surveillance practices, and which in turn benefits the economy. Online service providers and other businesses need the legal certainty that comes from the rule of law in order to operate globally. When national regulations comply with international human rights obligations, they both protect people's rights and bring economic benefits by more closely harmonizing regulations across borders. The US should build on existing commitments to digital rights, including through the Freedom Online Coalition,[4] and secure additional commitments to refrain from imposing Internet shutdowns, reject extralegal censorship, limit the use of surveillance technologies, and ensure access to end-to-end encrypted services.

The US should also promote opportunities for shared learning across governments, and with the involvement of human rights advocates, technical experts, and other civil society representatives, especially around emerging issues, including artificial intelligence. The IPEF process should coordinate with the variety of such learning and information-sharing fora that already exist across the US government, including the EU Technology Trade Council and the Freedom Online Coalition.

Finally, the US should recognize that nations sometimes have legitimate concerns that may impel them to adopt laws that threaten human rights, such as data and personnel localization mandates and requirements to undermine encryption. For the US to successfully promote the free flow of data, and reject overly restrictive national data protection laws that can serve as vehicles for censorship and surveillance, other nations must be able to have confidence that, for example, their citizens' data will be protected from corporate and government abuses when sent to the US.

Countering Digital Authoritarianism

This Committee is already familiar with the threat of digital authoritarianism presented by China's model of Internet regulation. China's government uses a variety of technical and legal practices to exert control over the Internet and the Chinese populace.[5] China engages in direct digital censorship, including through Internet shutdowns and through its decades-long project to build a "Great Firewall" that blocks outside information sources and enables the Chinese government to impose strict domestic

[4] *See* Freedom Online Coalition (last visited Mar. 12, 2022) [https://perma.cc/27Z8-PLXK].
[5] *See* United States International Trade Commission, *Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businesses*, (Feb. 2022) [hereinafter "US ITC report"] [https://perma.cc/W7KK-XGBK].

censorship policies. China also censors information through indirect means, including obligations for technology companies to store data within the country, to enable government access to user data.[6] Such requirements discourage foreign service providers from making information available in the country, and the threat of surveillance can exert a chilling effect on users. The Chinese government is notorious for its mass and discriminatory surveillance of the population, particularly of the Uighur community in Xinjiang province.[7] A lack of respect for human rights and weak rule of law in China mean that it is extremely difficult for US companies to operate responsibly in the country,[8] which has only further cemented the Chinese government's grip on its domestic communications network.

Unfortunately, the past three weeks have provided a stark example of the threats to human rights from digital authoritarianism, in the context of the Russian government's invasion of Ukraine. Bolstered by laws that give the government broad censorship and surveillance powers and that require foreign tech firms to locate personnel and data within the country, the Russian government has sought total control of the Russian people's access to information about the war the government is conducting.[9] The Russian government has throttled and ultimately blocked access to social media services that dared to attach fact-checks to state propaganda,[10] and has passed a new "fake news" law that prohibits anyone from "knowingly disseminating false information" about Russia's military, which is understood to include referring to its actions in Ukraine as an "invasion".[11] As a result, many media outlets have left the country, for fear of the safety of their personnel on the ground, and many online service providers have shuttered their services or are blocking access by Russian users, leaving the Russian people with few information alternatives to state propaganda and strengthening the government's control.[12]

Troublingly, these authoritarian tactics are already finding purchase in other nations, including in the Indo-Pacific region. The recent US International Trade Commission report, "Foreign Censorship Policies and Practices that Affect US Businesses" describes some of the growing digital censorship practices in India, Vietnam and Indonesia, among other countries.[13] It is vital that the US work with these nations and other leaders in the region to advance an affirmative vision for Internet governance grounded in an open, interoperable Internet free from digital censorship.

---

[6] *Id.* at 51.
[7] Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (May 1, 2019) [https://perma.cc/MG86-67B3].

[8] Global Network Initiative, *The Operation of the GNI Principles when Local Law Conflicts with Internationally Recognized Human Rights* (last visited Mar. 13, 2022) [https://perma.cc/5JJA-NZ6C].
[9] Human Rights Watch, *Russia: Growing Internet Isolation, Control, Censorship Authorities Regulate Infrastructure, Block Content* (June 18, 2020) [https://perma.cc/P7E7-SZAR].
[10] Dan Milmo, *Russia blocks access to Facebook and Twitter*, The Guardian (Mar. 4, 2022).
[11] Ann M. Simmons & Alexandra Bruell, *Russia Targets Media Outlets With 'Fake News' Law, Blocks Facebook*, Wall St. J. (Mar. 5, 2022) [https://perma.cc/Z9B3-9ENL].
[12] Guy Faulconbridge, *Russia fights back in information war with jail warning*, Reuters (Mar. 4, 2022) ; Rebecca MacKinnon, *The Invasion of Ukraine is Horrific. Cutting the Russian People Off From the Internet Could Make It Worse*, Tech Policy Press (Mar, 10, 2022) [https://perma.cc/D2MV-H6PZ].
[13] US ITC report, *supra* n.5

Digital Censorship Takes Many Forms

"Digital censorship" is direct or indirect state action that seeks to prevent or suppress online communication, or to punish online speakers, through laws, policies, or practices that are inconsistent with states' international human rights obligations. Digital censorship impedes both individuals' freedom of expression and their ability to receive information. Some forms are direct and overt, such as Internet shutdowns or laws prohibiting certain content. Other forms of government suppression of expression and information online are indirect, such as government pressure on content moderation processes through methods contrary to the rule of law and mandates to locate personnel in-country to increase the government's leverage over private companies. In this section, I discuss several forms of digital censorship and their economic consequences, including examples from the region (with country names in bold), as well as alternative, rights-respecting approaches that the US government could promote.

Internet shutdowns

A free, open, interconnected and interoperable Internet contributes to the enjoyment of human rights and freedoms by people around the world, including the rights to opinion and expression, assembly and association, public participation, privacy, and religious freedom and belief. Internet access is an essential prerequisite to full enjoyment of those rights in the digital age. However, as CDT and other human rights groups have noted, there is a disturbing trend of governments disrupting ICT services to calm unrest or thwart perceived threats.[14] State-sponsored network disruptions have grown from a few dozen in the years between 2008 and 2014 to 155 in 2020 alone.[15] According to UN Special Rapporteur Clement Voule, Internet shutdowns are now "'lasting longer' and 'becoming harder to detect.'"[16]

In **China**, the government uses Internet shutdowns to stifle dissent and control the flow of information to its people, often justified by claims of national security concerns.[17] In 2009, China shut down the Internet in Xinjiang, which had a population of 22 million people, for ten months in response to ethnic violence in the regional capital;[18] shutdowns have subsequently continued sporadically in that region.[19] More recently, China has also engaged in Internet shutdowns "to limit information related to the COVID-19 pandemic."[20]

---

[14] Michael Grimes & Emily Barabas, *Network Shutdowns*, Ctr. for Democracy & Tech. (Sept. 11, 2014) [https://perma.cc/GT5Z-H5A7].
[15] *Id.*; Access Now, *#KeepItOn* (last visited Mar. 13, 2022) [https://perma.cc/5DGJ-7L3Y].
[16] United Nations, *Internet shutdowns now 'entrenched' in certain regions, rights council hears*, UN News (July 1, 2021) [hereinafter "UN News"] [https://perma.cc/PSN7-53MW].
[17] Freedom House, *Freedom on the Net 2021 - China* (2021) [https://perma.cc/ZL3C-JAHG].
[18] *Id.*
[19] US ITC report, *supra* n.5, at 46.
[20] US ITC report, *supra* n.5, at 47.

When governments act directly or coercively to interrupt wireless service, they are enacting a "prior restraint" on speech which in turn inevitably suppresses many innocent speakers' ability to communicate; this has been especially effective in countries which have few Internet providers, leaving them technically more vulnerable to such shutdowns.[21] Military conflicts and protests are often the impetus behind Internet shutdowns, including within the Indo-Pacific region. The **Indian** government has imposed more Internet shutdowns than any other country in the world, "with 121 shutdowns in 2019 and 109 shutdowns recorded in 2020," often in response to protests or military crackdowns, such as in the Jammu and Kashmir regions.[22] In **Myanmar**, intermittent shutdowns and disruptions began following a military takeover in 2021, depriving residents of access to the outside world and to information about rights abuses.[23] The **Indonesian** government has also repeatedly shut down the Internet in regions of the country because of protests.[24] In **Bangladesh**, authorities imposed an "Internet blackout" on a refugee camp that lasted 355 days, in response to a demonstration by the refugees.[25]

Internet shutdowns demonstrate extreme vulnerability of mobile and Internet access companies to governmental pressure. These shutdowns harm human rights, and they are all the more concerning during the COVID-19 pandemic, because they "limit[] people's ability to obtain timely information about the pandemic or use digital tools to access health care, education, and other necessary services."[26]

In addition, Internet shutdowns have lasting economic effects, resulting from a myriad of impacts. Experts estimate that these costs add up to billions of dollars each year. For example, a report by Brookings conservatively estimated that the global economy lost $2.4 billion as a result of Internet shutdowns in 2015.[27] According to this analysis, India alone lost nearly $1 billion in 2015 because of its repeated Internet shutdowns.[28] More recently, a report based on the NetBlocks Cost of Shutdown Tool—which estimates the economic impact of an Internet disruption, mobile data outage or app restriction using indicators from the World Bank, ITU, Eurostat and US Census[29]—estimated that Internet shutdowns cost the economy $5.45 billion in 2021 and has already cost the economy $1.2 billion in 2022.[30]

---

[21] Emma Llansó, *CDT to FCC: Wireless Shutdowns Are Never the Right Choice*, Ctr. for Democracy & Tech. (May 1, 2012) [https://perma.cc/V53Z-KAX6].
[22] US ITC report, *supra* n.5, at 46; Adrian Shabaz & Allie Funk, *Information Isolation: Censoring the COVID-19 Outbreak*, Freedom House (2020) [https://perma.cc/FFL9-S7KM]; Software Freedom Law Center, *Internet Shutdowns* (2022) [https://perma.cc/ASS5-QSV3].
[23] Access Now, *Update: internet access, censorship, and the Myanmar coup* (Feb. 16, 2022) [https://perma.cc/MSX3-YPCA].
[24] Access Now, *Court rules the internet shutdowns in Papua and West Papua were illegal* (June 3, 2020) [https://perma.cc/4RWK-AN92]; Natalia Krapiva et al., *Indonesians seek justice after internet shutdown*, Access Now (May 13, 2020) [https://perma.cc/CM2H-QMN8].
[25] UN News, *supra* n.16
[26] Shabaz & Funk, *supra* n.22.
[27] Darrell M. West, *Internet shutdowns cost countries $2.4 billion last year*, Ctr. for Tech. Innovation at Brookings (Oct. 2016) [https://perma.cc/5N9L-GXLV].
[28] *Id.*
[29] NetBlocks, *Cost of Shutdown Tool* (2022) [https://perma.cc/JZN4-KN33].
[30] Samuel Woodhams & Simon Migliano, *Government Internet Shutdowns Have Cost Over $18 Billion Since 2019*, Top10VPN (Mar. 9, 2022) [https://perma.cc/R6KR-EPXA].

Requiring online service providers to determine the legality of speech

Intermediary liability laws, which establish whether and in what circumstances online service providers (or "intermediaries") face liability for hosting, transmitting, or otherwise enabling access to illegal user-generated content, are another tool that governments can use for direct or indirect digital censorship. Intermediary liability frameworks may take the form of broad, unconditional shields from liability[31] or conditional notice-and-action regimes that specify requirements intermediaries must meet upon being notified of illegal content, in order to maintain their statutory safe harbor from liability.[32]

There is currently considerable debate about the optimal contours of intermediary liability frameworks in the US and many other countries around the world.[33] However, intermediary liability frameworks that require or incentivize intermediaries to censor online content that is not illegal pose significant risk to freedom of expression. Some intermediary liability laws require private companies, rather than courts, to make determinations about whether specific user-generated content is illegal. These laws may also allow non-judicial authorities to declare content illegal, which circumvents the rule of law and international human rights standards.[34] One of the most notorious examples of this is the **Chinese** model, in which intermediaries are provided with extensive lists of prohibited content and required to actively police their services for it.[35]

Nevertheless, many governments around the world—including in the Indo-Pacific region—have adopted or proposed regulations that would require service providers to evaluate whether content is illegal after receiving a notification from an average user, or require providers to remove content pursuant to an order from a non-judicial government agency—or risk facing liability for the content themselves. Such laws will result in the erroneous removal of lawful speech. Users and non-judicial government agencies may accidentally misuse or purposely abuse notices by reporting content that is not actually illegal, spurring intermediaries to remove content rather than risk facing liability for it.

For example, in **India**, the 2021 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (the Indian Intermediary Rules) require online services to remove illegal content within thirty-six hours of receiving an order from a government agency—not necessarily a judge.[36] Online services must also remove certain categories of content, including sexually explicit material,

---

[31] *See, e.g.*, 47 U.S.C. § 230.
[32] *See, e.g.,* 17 U.S.C. § 512; European Union, Directive on Electronic Commerce, Directive 2000/31/EC.
[33] The European Union, for example, is revising its intermediary liability laws in the forthcoming Digital Services Act, though the core notice-and-action framework of the E-Commerce Directive will persist.
[34] *See* David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council of the United Nations 19 (Aug. 17, 2018) (finding that governments should only restrict access to or remove content pursuant to the order of an impartial judicial body in order to remain consistent with international human rights principles) [https://perma.cc/N3LV-ZEBU].
[35] Freedom House, *Freedom on the Net 2020 - China* B2 (Oct. 2020) [https://perma.cc/29SK-7XWU].
[36] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(1)(d) [hereinafter "2021 Indian Intermediary Rules"].

within twenty-four hours of receiving a complaint from any user about the material.[37] The Indian Intermediary Rules are stringent and could lead to jail time for employees of online services who fail to comply with requests to take down illegal content.[38] CDT has warned that the rules "open[] the door for . . . authorities to seek the removal of speech for political or other inappropriate reasons—and the Indian government already has demonstrated it will walk through that door."[39] The Indian Intermediary Rules are likely to serve a model for other legislation in the region; **Bangladesh**, for example, has already proposed similar guidelines.[40]

Some countries have used concerns about online disinformation or so-called "fake news," coupled with intermediary liability regimes that do not require a court order determining the illegality of speech, to require intermediaries to remove user-generated content. For example, in **Singapore**, the Protection from Online Falsehoods and Manipulation Act (POFMA) "permits a single government minister to declare that information posted online is 'false,' and to order the content's 'correction' or removal if deemed to be in the public interest."[41] Companies that refuse to comply face steep fines, and individuals who violate the law can be jailed.[42] According to Human Rights Watch, "As of mid-2020, the government had invoked POFMA more than 50 times, primarily against people or publications that criticized the government or its policies."[43] After one instance in which government officials ordered Facebook to block access to a blog post critical of the government's response to the COVID-19 pandemic, the company argued that the order was "disproportionate and contradict[s] the government's claim that POFMA would not be used as a censorship tool."[44]

Short time-frames for content removal

Another concerning liability trend involves laws or regulations that obligate providers to remove content on sharply abbreviated timelines—often within hours. These laws discourage companies from closely scrutinizing government or user demands to remove content and push them to err on the side of quickly removing content. Laws with short deadlines for content removals may also effectively require, or at least strongly encourage, intermediaries to use automated technologies to detect, filter, and remove

---

[37] Id., Rule 3(2)(b).
[38] Namrata Maheshwari & Emma Llansó, *Part 1: New Intermediary Rules in India Imperil Free Expression, Privacy and Security*, Ctr. for Democracy & Tech. (May 25, 2021) [https://perma.cc/WLZ4-D4DK]; *see also* Global Network Initiative, *GNI Analysis: Information Technology Rules Put Rights at Risk in India* (Mar. 30, 2021) [https://perma.cc/W2TG-B8M5] (explaining that failure to comply with the new intermediary rules can lead to a loss of safe harbor protections under the IT Act and ultimately result in prison terms of up to seven years for employees based in India).
[39] Maheshwari & Llanso, *supra* n.38.
[40] Mitaksh, *Bangladesh Releases Draft Rules To Regulate OTT Platforms, Modelled [sic] On India's IT Rules*, MediaNama (Feb. 9, 2022) [https://perma.cc/83WP-86YP].
[41] Human Rights Watch, *Singapore: 'Fake News' Law Curtails Speech* (Jan. 13, 2021) [hereinafter "HRW, Singapore"] [https://perma.cc/9P6L-TZB6].
[42] Ashley Westerman, *'Fake News' Law Goes Into Effect In Singapore, Worrying Free Speech Advocates*, NPR (Oct. 2, 2019) [https://perma.cc/2TJU-8HWM].
[43] HRW, Singapore, *supra* n.41.
[44] Reuters Staff, *Facebook says 'deeply concerned' about Singapore's order to block page*, Reuters (Feb. 18, 2020) [https://perma.cc/2VJX-RFCM].

content, with often disastrous impacts for users' freedom of expression. Despite recent advances in machine learning and artificial intelligence, automated content analysis techniques have significant limitations that create risks to human rights.[45]

Laws discouraging scrutiny of removal demands and encouraging the use of automated content analysis tools through brief timeframes for content removals are unfortunately proliferating in the Indo-Pacific region.[46] For example, the 2021 **Indian** Intermediary Rules require that intermediaries remove content within 36 hours after receiving a government order and that they remove certain other categories of content within 24 hours.[47] Similarly, in **Australia**, the new Online Safety Act requires providers to remove content sanctioned by the eSafety Commissioner within 24 hours.[48] And in **Indonesia**, electronic system operators could be required to remove prohibited content within just four hours after receiving notice from authorities, in urgent situations.[49] In **Thailand**, users can report banned content to intermediaries, and intermediaries "must remove flagged content within seven days for alleged false or distorted information, within three days for alleged pornographic content, and within 24 hours for an alleged national security threat."[50]

Weak intermediary liability regimes that can be leveraged for digital censorship not only impact users rights; they also impose economic costs. Given the high volume of user-generated content online and correspondingly high volume of content reported as illegal or violating a company's Terms of Service, it can be extremely costly for online intermediaries to actively monitor content, make decisions about the legality or illegality of content, and evaluate content under strict time frames to determine whether or not it should be removed.[51] Laws that require intermediaries to undertake these efforts—or face litigation costs or steep fines—serve as a barrier to entry to new intermediaries, stymying competition and growth. In addition, intermediaries that are unable or unwilling to comply with intermediary liability regimes that require them to invest huge amounts of resources may cease operating in a country altogether, depriving local users of online services that allow them to communicate with investors or customers, buy and sell goods, and engage in other economic activity.

---

[45] *See* Carey Shenkman et al., *Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis*, Ctr. for Democracy & Tech. 22-24 (2021) [https://perma.cc/XM4B-RLAY].
[46] Such laws and policies are not unique to the region: the European Union's Code of Conduct on Countering Illegal Hate Speech Online calls for participating companies to review content takedown requests from "trusted flaggers" within 24 hours. *EU: European Commission's Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision*, ARTICLE 19 (June 2016) [https://perma.cc/J8UV-TH8P]. Germany's NetzDG imposes a 24-hour timeline on providers to remove "manifestly" unlawful content, and illegal content that is not manifestly unlawful must be removed within seven days. NetzDG, Article 1§3(2)2-3.
[47] 2021 Indian Intermediary Rules, *supra* n.36, Rule 3(1)(d); *Id.*, Rule 3(2)(b).
[48] Freedom House, *Freedom on the Net 2021 - Australia* (2021) [https://perma.cc/T4LW-HYGA]; eSafety Commissioner, *Online Safety Act of 2021 Fact Sheet* (January 2022) [.
[49] Freedom House, *Freedom on the Net 2021 - Indonesia* (2021) [https://perma.cc/7YFC-YD5L].
[50] Freedom House, *Freedom on the Net 2021 - Thailand* (2021) [https://perma.cc/26V3-686V].
[51] Katie Schoolov, *Why content moderation costs billions and is so tricky for Facebook, Twitter, YouTube and others*, CNBC (Feb. 27, 2021) [https://perma.cc/L3SF-Z2XJ].

Manipulation of content moderation processes by state actors

Governments around the world are increasingly relying on service providers' own content policies to obtain removal of online content or accounts. Rather than challenging content in court as a violation of law, the government flags and reports it to the provider for removal on the basis that the content violates the provider's Terms of Service. In some countries, governments have formalized Terms of Service referrals using Internet Referral Units, which are government entities formed to flag user-generated content directly to the service provider that hosts it, often using the provider's own content-flagging mechanisms, so the provider will remove the content under its Terms of Service.[52]

Manipulation of private companies' content moderation processes are contrary to rule of law principles and allow governments to leverage providers' Terms of Service to censor online speech of which they disapprove. Terms of Service may prohibit a variety of types of speech, including far more speech than that which is prohibited by law. As a result, governments can use providers' Terms of Service to obtain removal of legal content, including content that cannot be made illegal consistent with international human rights standards. Government actors may also selectively target speech prohibited by providers' Terms of Service to censor speech based on viewpoint or content. In addition, government referrals can be coercive, exerting significant pressure on a provider to remove content "voluntarily" under its own Terms of Service. And, in some countries, providers face mandatory regulations for refusing to comply with government removal requests[53] or can be stripped of liability protection for user-generated content based on a government notification.[54]

Governments have used these Terms of Service referrals to target critics, rivals, or activists. For example, Amnesty International has reported that the **Vietnamese** government engages in "mass reporting campaigns" in which it relies on social media sites community reporting functions to have "large numbers of users . . . simultaneously 'report' a particular account or specific content with the aim of having it deleted or suspended by social media companies on the basis of it violating community standards."[55] According to news reports, the Vietnamese government has used the mass reporting technique to target journalists and human rights activists on Facebook."[56]

---

[52] Jason Pielemeier & Chris Sheehy, *Understanding the Human Rights Risks Associated with Internet Referral Units*, VOX-Pol (Mar. 26, 2020) [https://perma.cc/CC5Q-PF4L].
[53] Tomer Shadmy & Yuval Shany, *Protection Gaps in Public Law Governing Cyberspace: Israel's High Court's Decision on Government-Initiated Takedown Requests*, Lawfare (Apr. 23, 2021) [https://perma.cc/F4HX-LPPE] (stating that the Israeli Cyber Unit "has the power to subject the online platforms to mandatory regulations should they systematically refuse to comply with its takedown requests").
[54] Jim Killock, *Informal Internet Censorship: The Counter Terrorism Internet Referral Unit (CTIRU)*, Open Rights Group (Mar. 5, 2019) [https://perma.cc/LWM2-VTUD] (describing the impact of detailed notification under the E-Commerce Directive on content hosts' "actual knowledge" of criminal content and subsequent potential liability for that content).
[55] *'Let Us Breathe!': Censorship and Criminalization of Online Expression in Viet Nam*, Amnesty Int'l 53 (2020) [https://perma.cc/D88L-69CA].
[56] Russel Brandom, *Facebook's Report Abuse button has become a tool of global oppression*, The Verge (Sept. 2, 2014).

Local-presence requirements or "personnel localization"

Legal requirements that Internet companies locate personnel in particular country—known as "personnel localization" but sometimes referred to as "hostage provisions"[57]—are another mechanism through which states indirectly exert control over online speech. Personnel localization requirements make it harder for intermediaries to resist abusive government demands to shut down the Internet or to remove particular websites or user-generated content, because of the threat that failure to comply will result in punishment, including imprisonment, of the local personnel.

Recent events in **Myanmar** demonstrate how countries can use the presence of personnel in-country to exert control over communications intermediaries. Following the 2021 coup d'état, and demands by military leaders to shut down the Internet, block certain websites, and activate communications-intercept equipment,[58] Telenor Group decided to sell Telenor Myanmar.[59] The sale has yet to be formally approved by authorities in Myanmar, and as of February 2022, Myanmar had prohibited some Telenor staff, including a Telenor executive who is a Norwegian citizen, from leaving the country.[60] According to Telenor's CEO, "The authorities say that they want to have leading Telenor employees on the ground as long as they have not clarified whether we will be allowed to sell the business or not."[61]

Other countries in the Indo-Pacific region have required personnel localization by law or regulation. For example, the **Indian** Intermediary Rules require certain social media companies to have at least three responsible company employees resident in India, including a Chief Compliance Officer (CCO).[62] The CCO must be a "key managerial personnel from the company" and is personally liable for the company's failure to comply with the rule's requirements regarding content removals, facing penalties of up to seven years in prison and significant fines for noncompliance.[63] As the Software Freedom Law Center, India has explained, the personnel localization requirement poses significant financial and operational barriers to smaller companies operating within India and may mean that smaller or nonprofit companies, like encrypted messaging service Signal, cannot offer their services in India.[64]

---

[57] *GNI Submission to European Commission Consultation on the Digital Services Act*, Global Network Initiative (Apr. 1, 2021) [https://perma.cc/2JRT-YECV].
[58] Telenor, *Updates on Telenor in Myanmar* (Feb. 28, 2022) [https://perma.cc/2L7Z-STW5].
[59] *Id.* This decision raised human rights concerns because of links between the companies to which Telenor Myanmar is to be sold to the ruling military junta. Access Now, *As Myanmar junta extends control over telcos, surveillance and privacy risks increase* (Jan. 24, 2022) [https://perma.cc/VSU5-G6X7].
[60] Gregers Møller, *Norwegian Telenor leader is denied departure from Myanmar*, ScandAsia (Feb. 28, 2022) [https://perma.cc/6HJT-HD9S].
[61] *Id.*
[62] Maheshwari & Llansó, *supra* n.38; *Letter to MeitY and GNI Analysis of the IT Rules*, Global Network Initiative (Mar. 30, 2021) [https://perma.cc/998K-6R4C].
[63] This is not an idle threat; even before the effective date of the new rules, India threatened to jail employees of Twitter, Facebook, and WhatsApp for their failure to comply with takedown requests related to protests by Indian farmers against the government. See Jeff Horowitz & Newley Purnell, *India Threatens Jail for Facebook, WhatsApp and Twitter Employees*, Wall St. J. (Mar. 5, 2021) [https://perma.cc/W5V7-JPAP].
[64] *Analysis of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021*, Software Freedom Law Center, India (Feb. 27, 2021) [https://perma.cc/2FMZ-83MA].

Recommendations for combatting digital censorship in the Indo-Pacific

As Congress consults with the administration on the IPEF, CDT respectfully recommends that it prioritize adherence to international human rights standards and the rule of law, as key pillars of a sustainable, rights-respecting digital economy. International human rights standards could be incorporated into the IPEF, for example, through shared principles that articulate a fundamental commitment to freedom of expression online and state that efforts to regulate online speech must be grounded in human rights and the rule of law. The US should build on the work of the Freedom Online Coalition, which includes Australia, Japan, and New Zealand, and encourage additional states in the region to commit to join the coalition, engage in its diplomatic coordination function, and endorse its many joint statements regarding Internet freedom and human rights.[65]

The US should also take the opportunity in IPEF discussions to emphasize the importance of participatory policy-making processes that enable human rights defenders, technical experts, and other members of civil society to engage meaningfully. The US should seek commitments from other states to engage in multistakeholder consultation around issues of online content regulation and support civil society participation in policymaking processes. The US should also urge nations in the region to make use of existing subject-specific multistakeholder initiatives, such as the Christchurch Call to Action,[66] as fora for discussion, shared learning, and addressing global challenges within a framework that champions human rights and an open Internet.

In addition, the US should provide sustained funding for human rights-protecting technology and seek commitments to do the same from other nations engaged in the IPEF discussions. Moreover, the US should seek commitments from other nations not to interfere with individuals' use of critical privacy-enhancing and censorship-circumvention tools such as end-to-end encrypted services and virtual private networks (VPNs). As discussed in the next section, such tools are vital to people's ability to use the Internet and digital services for their own economic benefit and the enjoyment of their human rights.

Human Rights Risks of Surveillance, Impeding the Free Flow of Data, and Emerging Technologies

Threatening access to end-to-end encrypted services

In addition to countering digital censorship, digital trade discussions present the opportunity to address the human rights risks associated with surveillance, threats to data privacy, and emerging technologies. A top priority should be ensuring access to end-to-end encrypted services, which are essential to preserving individuals' communications privacy and enabling them to fully participate in the digital

[65] *See* Freedom Online Coalition (last visited Mar. 12, 2022) [https://perma.cc/27Z8-PLXK].
[66] *See* Christchurch Call (last visited Mar. 12, 2022) [https://perma.cc/XJ8M-ABFM].

economy. The Russian government's invasion of Ukraine is only the most recent reminder of how critical it is for journalists, activists, businesses, and everyday people to be able to communicate privately and securely, without fear of reprisal. Encryption is essential, not only in times of war, but for everyday activities such as reading the news, banking, exchanging business information, making purchases, running a small business, and communicating with loved ones—knowing that your data is secured from prying eyes.[67]

Unfortunately, a number of countries in the Indo-Pacific implement restrictions on people's access to strong encryption.[68] The **Indian** Intermediary Rules mandate "traceability" of online communications, requiring that intermediaries with more than 5 million registered users be able to identify and disclose the "first originator" of any information they carry.[69] Though the Indian government has proposed several methods for complying with this obligation, none of these methods would maintain the guaran-tees of privacy and security that users expect from services that are encrypted end-to-end. **Australian** law jeopardizes access to encryption in a different way, by permitting the Attorney General to issue "technical capability notices" that effectively require communications service providers to build back doors into their services to enable the government to surveil the communications of specific individuals.[70]

The US should strongly support individuals' access to end-to-end encrypted services and should seek commitments from other governments to do the same. The US should reject any proposals that reference exceptions or limitations to encryption, *e.g.,* to enable law enforcement access to content or to require certain forms of content moderation on encrypted messaging services. Instead, the US should work with other nations through the IPEF to share information about methods of investigation and approaches to law enforcement that do not require investigators to undermine these key security technologies. The US should also address underlying challenges to cross-border investigations by updating its own legal frameworks (see below).

Surveillance tools and surveillance-for-hire

Another threat to individuals' privacy is the growing availability of powerful surveillance technologies for government and private use, which threatens individuals' privacy and can subject them to arbitrary and discriminatory decision-making. For example, facial recognition technology (FRT) is increasingly in demand by law enforcement and administrative agencies in the US and in the Indo-Pacific region,[71]

---

[67] See David Kaye, *Report on encryption, anonymity, and the human rights framework*, United Nations Office of the High Commissioner on Human Rights (May 22, 2015) [https://perma.cc/5VBJ-3L8P].
[68] Global Partners Digital, *World map of encryption laws and policies* (last visited Mar. 12, 2022) [https://perma.cc/HP5K-4QKF].
[69] Namrata Maheshwari & Gregory Nojeim, *Part 2: New Intermediary Rules in India Imperil Free Expression, Privacy and Security*, Ctr. for Democracy & Tech. (June 4, 2021) [https://perma.cc/B7TQ-4YFP].
[70] Stilgherrian, *The Encryption Debate in Australia: 2021 Update*, Carnegie Endowment for International Peace (Mar. 31, 2021) [https://perma.cc/C8E3-WP68].
[71] Paul Bischoff, *Facial recognition technology (FRT): 100 countries analyzed*, CompariTech (June 8, 2021) [https://perma.cc/F75G-STPT].

despite the risk of biased and discriminatory policing that FRT enables.[72] Project Panoptic is monitoring at least 97 facial recognition technology systems in use across the **Indian** government,[73] and in **Japan**, FRT is used by law enforcement, commercial entities, and will be integrated into the national ID card.[74] In addition, the surveillance-for-hire industry presents a substantial threat through which private actors can use invasive software tools and other data collection strategies to target individuals. The Pegasus Project revealed the scale of this problem, identifying at least 180 journalists in 20 countries who were selected for potential targeting with NSO spyware from 2016-2021. A coalition of over 150 civil society organizations and independent experts have called on governments to regulate the export, sale and use of surveillance technology.[75]

The US has put NSO Group and others on the "entity list" because of the sale of surveillance tools to repressive governments,[76] and should seek commitments from governments in the Indo-Pacific region to do likewise. The US should also pursue shared principles condemning the use of spyware technologies and affirming the obligation of states to regulate the export, sale and use of such tools. It should seek commitments to investigate export licenses granted for surveillance technology; revoke marketing and export licenses where appropriate; implement procurement standards restricting government contracts for surveillance technology and services to only those companies which demonstrate that they respect human rights in line with well-established principles; and provide capacity building assistance to third countries to support multilateral export control regimes. Such efforts should complement, or ideally enhance, the Export Controls and Human Rights Initiative being developed in connection with the Summit for Democracy and any related efforts taking place within the US-EU Tech and Trade Council.

Barriers to the free flow of data

In general, the US should prioritize maintaining the free flow of data across borders in the region and worldwide. The global digital economy depends on the free flow of data, which enables people to access information and education, engage in financial transactions, and connect with other people; it

---

[72] Amy K. Lehr & William Crumpler, *Facing the Risk: Mapping the Human Rights Risks in the Development and Deployment of Facial Recognition Technology*, Ctr. for Strategic & Int'l Studies (July 27, 2021) [https://perma.cc/E4Z9-92EZ]. CDT has called for a federal moratorium on the use of FRT. Letter from Algorithmic Justice League et al., to the Honorable Mitch McConnell et al. (July 1, 2021) [https://perma.cc/NFN9-MLKR].

[73] Project Panoptic, *Facial Recognition Systems in India* (last visited Mar. 12, 2022) [https://perma.cc/6U2Q-8W79]; Anushka Jain, *The tech vs privacy face-off*, Forbes India (Aug. 24, 2021) [https://perma.cc/LDX7-8HYR]; Prabhjote Gill, *India is ramping up the use of facial recognition to track down individuals without any laws to keep track of how this technology is being used*, Business Insider India (Feb. 10, 2021) [https://perma.cc/6AXS-JSU4].

[74] *Japan's police introduce facial recognition system in criminal probes*, Japan Times (Sept. 13, 2020) [https://perma.cc/Q4PD-G34A]; *Japan's face recognition technology confronted by challenges in handling personal data*, The Japan News (June 23, 2021) [https://perma.cc/3M44-FDW6?type=image]; Alessandro Mascellino, *Japanese government selects SAFR face biometrics for in-person service access*, Biometric Update (Oct. 29, 2021) [https://perma.cc/ARV2-H8WE].

[75] Gregory Nojeim & Sharon Bradford Franklin, *CDT Joins Civil Society Orgs and Independent Experts Calling for Investigation and Regulation of the Sale, Transfer and Use of Surveillance Technology*, Ctr. for Democracy & Tech. (July 27, 2021) [https://perma.cc/L52M-ZNPJ].

[76] Drew Harwell et al., *Biden administration blacklists NSO Group over Pegasus spyware*, Wash. Post (Nov. 3, 2021) [https://perma.cc/26LD-SQ3L].

also enables businesses of every size to attract and serve customers around the world. Well-intentioned measures designed to protect consumers in a particular jurisdiction, such as data protection laws, data localization laws, and laws mandating government access to communications data in order to fight crime, can have the inadvertent effect of restricting data flows and contributing to the splintering of the Internet.

The US should pursue a strategy in the Indo-Pacific region that recognizes the importance of cross-border data flows as an essential component of the digital economy and that addresses the underlying concerns that motivate restrictive measures, such as data localization mandates, that threaten human rights. For example, the US should leverage the requirements of the CLOUD Act, which sets certain standards that a foreign government's surveillance laws must meet in order to gain access to communications content held by US companies. The CLOUD Act empowers the US to seek specific improvements in other nations' substantive and procedural protections for privacy and civil liberties in their communications surveillance laws, and presents a compelling alternative approach to data localization mandates for enabling foreign law enforcement access to communications data for legitimate purposes.

The US should also pursue agreement with governments in the region on shared principles that countries should adopt strong comprehensive privacy protections that protect all individuals' data, have in place an effective enforcement regime that provides meaningful redress, and avoid imposing data localization requirements that restrict beneficial data flows or local data "mirroring" requirements in the name of protecting privacy. This is yet another reason for Congress to prioritize passing federal privacy legislation and reforming US surveillance law: The lack of a strong federal privacy law in the US, along with concerns about the scope of the US government's surveillance powers,[77] fuels the drive for data localization in the region. For the US to successfully promote the free flow of data, and reject overly restrictive national data protection laws that can serve as vehicles for censorship and surveillance, other nations must be able to have confidence that their citizens' data will be protected from corporate and government abuses when sent to the US.

Emerging technologies

Finally, there are a wide range of emerging issues in the digital sphere that will be relevant to discussions of the digital economy. New surveillance technologies and data-driven assessment tools are making it easier for companies to monitor workers in the workplace, and make inferences about employees based on a wide variety of data points. Examples include the use of AI in hiring or promotion decisions; "bossware" that closely monitors workers' activities to assess performance and efficiency in both factories and office environments;[78] and software that analyzes workers' social media

[77] Gregory Nojeim, *Schrems II and the Need for Intelligence Surveillance Reform*, Ctr. for Democracy & Tech. (Jan. 13, 2021) [https://perma.cc/G7XH-Q75T].

[78] *See* Matt Scherer & Lydia X.Z. Brown, *Warning: Bossware May Be Hazardous to Your Health*, Ctr. for Democracy & Tech. (July 24, 2021) [https://perma.cc/S2MJ-JT9L].

activities. These tools present clear risks for workers' privacy, autonomy, ability to organize, and physical and mental safety.

The US should raise awareness about these threats and demonstrate its commitment to protecting workers' interests. Potential strategies could include pursuing shared principles that recognize the risks of work-related surveillance tools for workers' privacy, autonomy, ability to organize, and physical and mental safety. These could articulate clear red lines on certain topics, like the extension of surveillance technology outside the workplace, or the use of surveillance technology to impede worker organizing. The US should also consider developing a cooperative mechanism or engaging in information sharing between the labor departments of participating nations about the types of technologies being deployed to monitor and evaluate workers, their prevalence and impacts, and approaches to regulation and/or oversight. These efforts would overcome the significant information asymmetry that makes it hard for workers, advocates and governments to engage in oversight of such tools.

More broadly, across the US government and in other countries, there is a growing awareness that AI technology can bring not only new opportunities, but also risks – including the risk that AI or data-driven decisionmaking in fields such as employment, lending, housing, or access to public benefits can reinforce existing biases in society, or make decisions in a way that evades public scrutiny and accountability.

The US could use the IPEF as a forum to raise awareness about these issues, share information about potential regulatory responses, and articulate shared principles recognizing these concerns. This could include pursuing commitments for countries to adhere to the OECD AI Principles, to which many IPEF target nations already subscribe.[79] The US should also pursue principles that recognize the potential for AI, while clearly warning about the risks in various use cases. These should set clear red lines on the most dangerous use cases of AI, along the lines of the US-EU TTC's condemnation of social scoring systems.

The US should also engage in information-sharing with governments in the region about risks that arise in different AI use cases, including countries' own experience deploying the technologies and specific ways to address those risks. This could include information-sharing sessions that bring in experts from civil society and the private sector to share knowledge on how to conduct or require meaningful audits and impact assessments; approaches to transparency and explanations regarding how AI systems are used; processes to improve procurement and public accountability around government use of AI in the administration of public benefits; and ways to evaluate the appropriateness of using AI (such as facial recognition technology) for law enforcement purposes. One good model of this sort of information-sharing is the Freedom Online Coalition's Task Force on Artificial Intelligence and Human Rights (T-FAIR), which meets regularly with member governments, experts from civil society, members

[79] *Given the principles' high level nature, these should be seen as a baseline to improve upon with more specific commitments and frameworks for cooperation/information sharing.*

of the private sector, and other stakeholders to deepen our collective understanding on topics such as the use of automation in content moderation, human rights considerations around facial recognition technology, and the design and deployment of algorithms by online services. Information-sharing efforts under IPEF should also build on efforts the Administration is developing as part of the US-EU TTC, and should be synced with US domestic efforts currently being led by OSTP, NIST, EEOC, CFPB, ACUS and other agencies.

* * *

The Internet and associated technologies are the backbone of the global economy. Only an open, interconnected, stable, and secure Internet can foster the fullest level of economic benefit for the US and its trading partners; this is best achieved and safeguarded by legal systems that respect human rights and the rule of law. There are a great many challenges to digital rights in the Indo-Pacific region, not least of which is the growing influence of the authoritarian model of Internet regulation promoted by the Chinese government. The United States should advance rights-respecting Internet law and policy through its trade engagements and the IPEF.