ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

March 3, 2023
Office of the United Nations High Commissioner for Human Rights
United Nations Office
CH 1211 Geneva 10
Switzerland

Re: Call for inputs: "The relationship between human rights and technical standard-setting processes for new and emerging digital technologies."

To the Office of the United Nations High Commissioner for Human Rights,

This submission represents the views of the Information Technology and Innovation Foundation (ITIF), a non-profit, non-partisan think tank focused on the intersection of technological innovation and public policy.

If you have any questions, please do not hesitate to contact me at ncory@itif.org.

Sincerely,

Nigel Cory

Associate Director, Trade Policy, The Information Technology and Innovation Foundation

OVERVIEW

The Office of the High Commissioner for Human Rights (OHCR's) inquiry into human rights and technical standard-setting processes for new and emerging digital technologies comes at an important time given China's growing role in technology development and standards setting. However, standards are not central to the issue. Countries with good—and bad—human rights records can and are imposing their own "values" on emerging technologies through domestic laws and regulations. OCHR should focus on engaging policymakers on these laws and regulations as this is the main vehicle for effecting change. China and other countries with poor human rights records are trying to influence international standard, but this is mainly at the International Telecommunications Union (ITU). OHCR's attention should be focused on the ITU as it is the venue for the most problematic standards proposals with clear and troubling human rights implications, especially relating to facial recognition and for a new centralized, state-directed Internet via the "New IP" initiative.

The OHCR's inquiry needs to be targeted as there are hundreds of SDOs and tens of thousands of standards that work as part of a system without any issues. This is due, in part, to the fact that, in 1995, most countries made legally binding commitments on principles and best practices for international standards through the World Trade Organization's (WTO) Technical Barriers to Trade Agreement (TBT), such as on the principles of openness, transparency, and consensus-based decision-making.[1] This submissions shows the considerable crossover between the role these principles play in ensuring countries don't use country-specific standards as a barrier to trade and how they can help identify and address international standards that raise human rights concerns. These principles act as a safeguard against problematic standards proposals from any one stakeholder or from a group of firms from a particular country.

OHCR's inquiry should be based on a clear understanding of what technical standards are and how they're made and used. Debates around values, human rights, and technical standards are often based on a poor understanding of technical standards. Standards are just one tool with a specific technical purpose. They help define how products and services work. Standards are not silver bullets for regulating technology. They were never designed to be jammed packed with requirements to address any and all related values and human rights concerns. That is the role of a country's laws and regulations. Furthermore, standards provide a voluntary tool that governments and firms don't have to use. Standards are also just one of many policy tools that governments can use to ensure reasonable and responsible laws and regulations for new and emerging technologies. Stakeholders with human rights concerns should engage countries' legislators and policymakers about their respective laws and regulations, as that is the proper venue and the vehicles for this (i.e., human rights concerns) debate. Laws and regulations provide both the framework for what SDOs develop and what standards a country decides to use.

The OHCR is not alone in paying growing attention to the nexus between technical standards and human rights given China's growing efforts to influence technical standards and its problematic domestic approach to both technical standards and human rights. For example, Article 23 of China's Standardization Law makes the national security nexus of standards work clear: "The State shall promote standards that encourage civil-military integration and … promote the use of advanced and appropriate civilian standards in the development of national defense and the military."[2] This centralized and state-driven approach is very different to how most other countries approach technical standards. For example, the U.S. approach to standardization is bottom-up: allowing open competition from the private sector in a free-market, multistakeholder fashion that resists central planning. This provides much greater openness and transparency, as well as competition and cooperation, for stakeholders to debate and develop technically focused standards (rather than politically motivated ones). The United States, United Kingdom, and European Union are particularly concerned about the focus of both the Chinese government and Chinese firms on international standards, as the former can coordinate the latter, while they're both able to provide inducements to other governments to build support for their standards proposals. No other country has China's ability to coordinate engagement on international standards by exerting pressures on foreign governments and its own firm alike, especially at the ITU.[3]

Human rights are clearly important and encompass a broad set of issues yet concerns about technical specifications tend to be isolated and at the ITU. The risk is this growing concern about standards, combined with a general misunderstanding about standards, leads to an overly broad response by OHCR, human rights advocates, and overly assertive governments who push to inject subjective issues into what is a technical process. Some human rights advocates may push for governments to play a more direct role in setting standards. The case of the ITU shows why this would be counterproductive. It's exactly due to the ITU's government membership (in contrast to transparent, consensus-based, and multistakeholder SDOs) that authoritarian governments can push standards that have clear and deleterious human rights implications.

This submission analyzes the importance of the WTO's principles for making international standards and how these provide a safeguard against problematic standards proposals. It then focuses on the issue of standards and values. It then focus on the ITU and the problematic standards proposals that get the most attention for obvious human rights concerns, including the "New IP" proposal and standards for facial recognition. It also details a historical case involving standards for deep packet inspection of Internet traffic. It analyzes how authoritarian governments use the ITU to advance human rights-infringing standards. These cases are important as they reflect the fact that authoritarian countries don't push these proposals in other SDOs (due to their open, transparent, and consensus-based governance). This submission concludes with a range of recommendations, including that human rights-respecting governments have both standards experts and human rights experts who know about standards processes, that they have an information sharing mechanism for local stakeholders, and that they coordinate better with likeminded partner countries to counter problematic standards proposals at the ITU.

WTO PRINCIPLES PROVIDE A SAFEGUARD AGAINST PROBLEMATIC STANDARDS PROPOSALS

The WTO's TBT agreement outlines how international standards should be based on the following principles: transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and the development dimension.[4] These principles support the good governance that acts as a guardrail against poor standards proposals or efforts to unduly influence the standards development process to get a standard that suits one potential firm or country, such as an authoritarian one.

The two most-cited examples (discussed later) about standards for new and emerging technologies involving clear and troubling human rights implications—facial recognition and "New IP"—have one thing in common: they were both considered at the ITU. The ITU claims it abides by the WTO principles, but in reality, it doesn't. Bringing these principles to life depends on governance and proper oversight, and the ITU doesn't do a great job here. Poor governance is why authoritarian governments can propose troubling standards at the ITU. It also raises the corresponding recommendation about why human rights-respecting countries need to be paying more attention at the ITU.

These ITU cases highlight the value of two key WTO principles: consensus and openness. Firstly, consensus voting is central to good governance at SDOs as it means no stakeholder group has special rights or privileges. No one firm/country can ram a standards proposal through, nor does any one stakeholder hold a veto over the process.

Secondly, the ITU is not truly open to outside participants. While notionally welcome at the ITU, in reality, industry participation is barely tolerated. Although companies can pay to participate in the standardization process as sector members, they cannot cast formal votes to decide which standards get adopted or not. Furthermore, draft ITU Telecommunication Standardization Sector (ITU-T) documents are available only to ITU members, meaning that the public lacks visibility into its standardization. This impacts both industry and civil society's ability to challenge problematic proposals. The reality is that many industries don't engage at the ITU as it is not a useful venue for standards discussions for the same reason why the ITU is a problematic forum for human rights-related proposals: governments propose bad technical standards. Authoritarian governments prefer the ITU exactly for this reason in that they can push politically motivated standards discussions and not face the same pushback and criticism that the same proposal would face in open and transparent international standards bodies. Instead, industry participants engage at other SDOs where discussions are technically based and open to genuine and good faith engagement. In many cases, ITU standards discussions are duplicative and unnecessary as these discussions are being considered in other SDOs.

The WTO principle of openness is critical to SDOs and their good governance. One does not hear about human rights-related concerns at the 3rd Generation Partnership Project (3GPP), the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), joint ISO-IEC technical committees, the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), or many other SDOs, as they're open to outside participation. They're also industry- and technically-directed (not government-directed) organizations and their governance provides guardrails against bad proposals. The openness of these and other SDOs also has a direct impact on the quality of standards as the entire standardization process, from initial proposal to final adoption, is open to anyone with relevant expertise who wants to comment and contribute. Only robust and useful technical standard survive the collective scrutiny of an SDO's membership.

For example, IETF has no formal membership requirements and is comprised of volunteers from government, the private sector, and civil society. IETF releases requests for comment that set and maintain basic, low-layer technical standards and norms for Internet protocols. These standards and norms are adopted by the Internet community including software developers and Internet service providers—not because they are binding, but because their contributors and the IETF itself have great influence.[5] This is why the predominant model of standards development for the Internet (as exemplified by the IETF) is based on open processes that stress technical excellence and bottom-up innovation. Any interested person (or organization) can suggest a new idea to be standardized, and the debate about its technical merits is open to the public. Through this process, the most innovative, technically sound proposals bubble up to the top and eventually become adopted as technical standards by the engineering community.

TECHNICAL STANDARDS ARE NOT THE SAME AS LAWS AND REGULATIONS.

Governments impose their values on emerging technologies through laws and regulations. OHCR and human rights advocates should engage legislators and policymakers about their respective laws and regulations as this is the proper venue for the debate about how to regulate technology. Standards provide instructions for how to engineer systems, services, and products. There are important differences between standards and laws/regulations when considering human rights and other issues raised by new and emerging technologies.

Firstly, international standards are voluntary, a country's laws and regulations are not. Governments and firms can simply decide not to use standards they don't like if there are clear human rights implications. For example, even if countries agreed to clearly problematic facial recognition or other standards at the ITU, countries and firms wouldn't have to use them. ITU standards are not mandatory. Russia, several Middle

Eastern countries, and others have tried (and thankfully failed) to make ITU recommendations mandatory for Internet technology companies and network operators to build into their products.

Which gets at an associated point about the voluntary nature of standards—they are only valuable and widely used if they're developed in an expert, technically driven process that is based on consensus. If firms and governments recognize that they're robust and useful tools to address a specific issue, they will use them. If China managed to influence an SDO to develop a facial recognition technology that clearly breached human rights concerns about ethnic profiling, for instance, the United States, United Kingdom, and any other country could simply choose not to accept, use, or reference that standard. At which point, the standard is essentially useless as firms wouldn't use it as they know it's not accepted in key markets.

The adoption of technical standards on the Internet has always been voluntary as it allows technology developers to decide how to package and build on standards within their products and services. Voluntary standards adoption plays an important role in underpinning ICTs and digital innovations like the Internet — that is, thriving, technically sound innovation, without permission from some central entity (like a government). In contrast, if governments were to mandate the use of specific standards, it would lock developers into that government's (or a group of governments') view of the Internet as it exists at a particular point in time. Innovation would supersede the pace at which governments would develop new standards. Since governments would be loath to constantly add new mandatory requirements to their countries' entire technology sectors, technology companies across the board would be wedded to outdated standards even when some of them would have otherwise been prepared to make upgrades.

Secondly, SDOs do not operate in a vacuum separate from policy debates about the human rights implications of their work and new and emerging technologies. On the contrary, SDOs are often ahead of the mainstream policy debate about new technologies and human rights concerns. For example, since 2016, IEEE has been developing a series of ethical standards around artificial intelligence (AI) that started before the conversation around human rights and AI became a mainstream concern. Several global standards bodies, including the IETF and W3C, have launched initiatives to incorporate privacy considerations into their work.[6] Key SDOs have made clear and early policy decisions concerning technologies and key human rights concerns, such as privacy. IETF stated that pervasive monitoring is a technical attack on privacy and should be mitigated in the design of IETF protocols.[7] Likewise, IETF opposed efforts to create encryption methods in Internet protocols that would have given governments unique, privileged access to the contents of otherwise encrypted communications. It also opposes efforts to restrict the use of encryption (such as via export controls).[8] IETF has long had a policy of not considering technical requirements for wiretapping in its work.[9]

THE ITU: FOCUS ON THE PROBLEMATIC PROPOSALS AND VENUE

The OHCR should focus on the ITU as it is the venue for most of the examples that drive the debate around standards and human rights. Standards discussions at the ITU attract legitimate concerns about the human rights implications of certain technologies. But this is because it is a government-membership based body. Having governments—the only formal decision-making members of the ITU—decide which standards technology companies must build into their products is problematic. It's not surprising then that allowing authoritarian governments to directly influence standards based on "their" view of human rights leads to standards that are both technically infeasible and highly problematic from a human rights perspective. Thankfully, the leader in this effort—China—have often proved ineffective as it struggles to build broad and genuine support for its proposals and often doesn't prepare well-supported and high-quality submissions. But this may change, which is why human rights-respecting governments and other stakeholders need to up their game at the ITU. This section details the most cited ITU standards from a human rights perspective.

China’s Effort to Use the ITU to Support a Centrally Managed Internet: The “New IP” Initiative

In 2019, Huawei officials proposed a new top-down, centralized design for Internet governance called “New IP [Internet Protocol].”[10] This centralized architecture would put vendors and state entities into a gatekeeping role, which obviously raises human rights concerns about privacy, censorship, and surveillance. China wanted to use New IP to initiate a broad digital economy discussion at the ITU (well beyond the scope of its usual work), but it knew if it led the initiative, it’d likely fail. It wanted the Asian bloc of countries at the ITU to jointly present the initiative, but China couldn’t get consensus among this group. So China got Malaysia to lead the effort. The case of New IP is indicative of the potential threat from one country (China) using all the tools it has to build a coalition to support technical standards that clearly impact human rights. For example, the Chinese government used government- and private sector-related information and communication technology (ICT) projects to build support in Africa for Huawei’s New IP proposal.

New IP is indicative of China and other authoritarian government efforts to expand the scope of the ITU’s work to include digital trade and the broader digital economy, even though the ITU’s jurisdiction does not include Internet architecture. ITU’s government membership format lends itself to efforts made by China and other authoritarian countries to try to make the ITU into a vehicle for a more centralized and state-controlled Internet and technology governance framework. New IP is an example of China’s pursuit of issue creep and forum shopping in taking issues that are normally discussed at the WTO and at technical, multistakeholder forums like the IETF and trying to put them on the ITU agenda (despite the fact the ITU has hitherto not been involved in standards-setting for Internet traffic and digital trade).

Thankfully, China was not successful in getting New IP adopted. Industry representatives identified the proposal as highly problematic and highlighted it to the U.S. government late in the process, which then finally acted. The United States, along with the European Union (EU), EU member states, and other countries worked together to squash the proposal. It’s important to note that the ITU, as in the institution itself, did not push back on the Chinese proposal. A takeaway from this case is that countries that value human rights need to pay attention to all the various ITU proposals and to ensure they have human rights and standards policy expertise in the room at the right time.

China and Facial Recognition Standards

In 2019, Chinese tech firms proposed controversial technical standards for facial recognition at the ITU. This case gets perhaps the most attention of any issue in terms of standards and human rights. Their standard stipulates a requirement to store detected facial features in a database, including race, skin color, face style, birthmarks, scars, and other demographic features. This obviously could be used for ethnic profiling, which is obviously concerning given China’s use of facial recognition in its genocide of ethnic Uighurs.[11] The standard’s suggested uses for facial recognition technology include the examination of people in public spaces by the police, confirmation of employee attendance at work, and the arrest of criminals, specifically by comparing “the country’s fugitive library with the local population library” to smoke out “local hiding criminal fugitives”.[12] Human rights lawyers criticized the proposal as crossing the line from technical specifications to policy recommendations, including outlining use cases and data requirements for facial recognition and other surveillance technologies.[13] In the context of the debate about facial recognition technology standards, the ITU study groups department stated that it is rare for civil society and consumer protection organizations to attend standards setting meetings.[14]

ITU and Deep Packet Inspection Standards

In 2012, the ITU approved a standard for deep packet inspection (DPI) that raised privacy concerns given the ability of governments to use it for surveillance.[15] The standard includes the option that DPI systems support the inspection of encrypted traffic, which is antithetical to most norms, policies, and laws concerning privacy of communications. The standard barely even acknowledges that there is a privacy risk at all. Furthermore, the ITU-T's technical work on DPI fails to acknowledge basic user interests in network security or to specify robust mitigations against security threats. It's unclear who actually uses this standard, which highlights the value of voluntary and technically driven standards. This case also highlights the risks of addressing cybersecurity issues through a closed, centralized body where ultimate authority rests with regulators and where technical experts and advocates cannot even access draft specifications.[16]

RECOMMENDATIONS

Below are some recommendations to the OHRC on the issue of human rights and technical standards.

Governments Need to Have the Right People Paying Attention

Governments that support human rights need to engage early, often, and for the duration of standards processes to be effective in ensuring that proposals at the ITU, ISO, IEC, and elsewhere are properly vetted for human rights concerns. Furthermore, human rights-respecting governments need to have the right mix of people in the room or on hand when standards discussions for new and emerging technologies with potential human rights implications are taking place. Standards specialists need to have human rights experts that understand the standards process on hand to call in when needed. Diverse government teams are clearly needed at the ITU, but also at the ISO/IEC, in ensuring national delegations have diverse membership. The United States generally does a good job at putting together diverse national committees for the ISO/IEC, but it's highly likely that many other countries don't do the same. In many governments, the left hand doesn't even know the right hand exists in that standards experts and human rights experts aren't connected.

Human Rights Expertise + Standards Expertise = Effective Engagement

Human rights experts won't make an impact at SDOs if they are not technically proficient. Other (non-ITU) SDOs are supportive of expanding their membership to stakeholders that are interested and effected by the standards they're developing. Academics, civil society, and human rights organizations could certainly increase participation at SDOs, but to contribute, they need to have the technical expertise to understand the underlying technology and the process for setting technical standards. While SDOs differ widely on their focus and each has its own rules, processes, and terminology, what is consistent is that discussions are technical in nature. All stakeholders need to be able to engage in an applied, technical sense. Stakeholders that engage on the basis of broad, rhetorical points about human rights will not influence the process. Decisions are made on the basis of technical merit, not normative arguments about values. In addition, human rights stakeholders must also recognize that they're just one of many stakeholders (the consensus principle of SDOs).

Human Rights-Respecting Governments Need to be Vigilant at the ITU

China and other authoritarian governments' ability to successfully advocate for their preferred approach to digital and technology governance at the ITU depends, in part, on an apathetic and passive membership. The United States and other human rights-respecting countries need to reengage across the board at this often bureaucratic, slow moving, and sometimes exasperating institution, and its myriad of committees and discussions, to ensure that each and every proposal is vetted for potential human rights or other concerns.

OHRC and Governments Should Support the WTO Principles and Open Participation at Standards Bodies

The ITU case highlights a question as to why similarly problematic proposals relating to new and emerging technologies and human rights haven't arisen from other SDOs. It's exactly due to the WTO principles and the good governance they support that other SDOs are able to identify, discuss, and reject proposals that are politically motivated. OHRC, other human rights advocacy organization, and governments should support the WTO principles for international standards making, especially open participation at standards bodies. Openness and other WTO principles are key differences between industry-led, technically focused processes and the ITU, where standards are more likely to be government-led.

A Government Takeover of Standards Setting Would be Counterproductive

Government intervention in international standards setting is not the answer to case-specific human rights concerns about technical standards. Standards discussions at the ITU have attracted legitimate concerns about the human rights implications of certain technologies exactly because of its government-based membership and voting. Having governments as the main decision makers at standards bodies lends itself to them injecting subjective, political concerns into the standards process in a way that does not happen at open and transparent international standards discussions.

Countries That Support Human Rights Need to be Better Informed and Coordinated on Technical Standards Discussions

Countries that defend human rights need to coordinate with likeminded partners about what is happening in the ITU, ISO/IEC, and the many other SDOs and where they need to pay attention and take potential joint action. If this were happening, problematic ITU standards proposals would have been identified and addressed much earlier than they have been recently. Such countries should also create information sharing mechanisms with industry and human rights experts to ensure they understand what is happening in standards setting bodies and where they need to potentially take action. Governments aren't involved in the vast majority of SDOs, so it's a matter of ensuring they have reporting mechanisms in place to inform them and direct their attention.

[1] "Principles for the Development of International Standards, Guides and Recommendations," World Trade Organization, https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm.

[2] "Standardization Law of the People's Republic of China (Revised Draft)," May 17, 2017, https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Links%20Within%20Stories/China%20Standardization%20Law_English%20translation_SESEC_5.17.2017.pdf.

[3] "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order," (National Bureau of Asian Research, March 1, 2022), "https://www.nbr.org/publication/chinas-digital-ambitions-a-global-strategy-to-supplant-the-liberal-order/.

[4] Ibid.

[5] Mallory Knodel, "The Privacy in the Protocol: Why Civil Society Needs to Pay Attention to the IETF," Freedom Online Coalition, https://freedomonlinecoalition.com/blog/the-privacy-in-the-protocol-why-civil-society-needs-to-pay-attention-to-the-ietf-by-mallory-knodel/

[6] “Privacy Considerations for Internet Protocols,” Network Working Group at IETF, July 16, 2012, https://datatracker.ietf.org/doc/html/draft-iab-privacy-considerations-03. “W3C Privacy Activity,” https://www.w3.org/standards/webdesign/privacy.

[7] “Pervasive Monitoring Is an Attack,” IETF, May, 2014, https://www.rfc-editor.org/rfc/rfc7258.

[8] “IAB and IESG Statement on Cryptographic Technology and the Internet,” August, 1996, https://datatracker.ietf.org/doc/rfc1984/.

[9] “IETF Policy on Wiretapping,” May, 2000, https://www.rfc-editor.org/rfc/rfc2804.

[10] Internet architecture has generally been the remit of the IETF. [Accessed via the Way Back Machine] “A Brief Introduction about New IP Research Initiative,’ Huawei, https://web.archive.org/web/20210705190300/https://www.huawei.com/us/technology-insights/industry-insights/innovation/new-ip; Madhumita Murgia and Anna Gross, “Inside China’s controversial mission to reinvent the internet,” *Financial Times,* March 27, 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f; Julia Voo and Rogier Creemers, “Report: China’s Role in Digital Standards for Emerging Technologies – Impacts on the Netherlands and Europe,” Leiden Asia Centre, May, 2021, https://leidenasiacentre.nl/report-chinas-role-in-digital-standards-for-emerging-technologies-impacts-on-the-netherlands-and-europe/.

[11] Drew Harwell and Eva Dou, “Huawei tested AI software that could recognize Uighur minorities and alert police, report says,” *Washington Post,* December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/; Johana Bhuiyan, “US sanctioned China’s top facial recognition firm over Uyghur concerns. It still raised millions,” *The Guardian,* January 7, 2022, https://www.theguardian.com/world/2022/jan/06/china-sensetime-facial-recognition-uyghur-surveillance-us-sanctions.

[12] Anna Gross and Madhumita Murgia, “Chinese tech groups shaping UN facial recognition standards,” *Financial Times,* December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

[13] Ibid.

[14] Ibid.

[15] "Requirements for Deep Packet Inspection in Next Generation Networks" or "Y.2770." Y.2770: https://www.itu.int/ITU-T/recommendations/rec.aspx?id=11566&lang=en. Y.2771: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12178; https://www.networkworld.com/article/2161782/itu-packet-inspection-standard-raises-privacy-concerns--says-cdt.html.

[16] Emma Llanso and Alissa Cooper, “Adoption of Traffic Sniffing Standard Fans WCIT Flames,” Center for Democracy and Technology, November 28, 2012, https://cdt.org/insights/adoption-of-traffic-sniffing-standard-fans-wcit-flames/.