Technical Standards and Human Rights: The case of New IP

Carolina Caeiro[a], Kate Jones[b] and Emily Taylor.[c]

[a]Chatam House, London, UK; [b] Diplomatic Studies Programme, University of Oxford, Chatham House, Oxford, UK; [c]Oxford Information Labs, Chatham House, Oxford, UK.

This unedited draft chapter is in peer review and will appear in a forthcoming volume, *Human Rights in a Changing World*, to be published by Chatham House and Brookings Institution Press. The opinions expressed in this publication are the responsibility of the author(s).

1. Introduction

Western governments are paying increased attention to technical standards and the ethical and human rights implications of emerging technologies. In the 2021 Digital and Technology Ministerial Declaration, G7 member countries created the 'Framework for Collaboration on Digital Technical Standards' which was subsequently endorsed by G7 leaders.[1] The framework referred to Internet protocols and technical standards for emerging technologies as areas that 'could affect shared values as open and democratic societies.'[2] Likewise, the UK government pledged to work with partners 'to ensure the rules and standards governing digital technologies are rooted in democratic values.'[3] Standards development --previously a niche field reserved to engineers-- is taking a leading role in government strategies.

This newly found attention appears directly linked to a set of proposals that China submitted for consideration within the Standardization Unit of the International Telecommunications Union Standardization Unit (ITU), the Geneva-based UN agency tasked with overseeing country-led international cooperation in the telecom sector. Introduced by Chinese delegations as 'New IP,'[4] the proposals would have resulted in the creation of a series of technical standards that would set the basis for a new, centralized Internet architecture. While it is unclear whether New IP and its associated technologies will progress as standards proposals, efforts to push for their standardization reveal a lot about China's ambitions. The country has openly stated that the rise of new technologies provides China the opportunity to 'seize the commanding heights of

[1] Cabinet Office, "Carbis Bay G7 Summit Communique," 2021 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1001128/Carbis_Bay_G7_Summit_Communique__PDF__430KB__25_pages_.pdf).
[2] G7 Information Center, "G7 Digital and Technology Track – Annex 1," 2021 (www.g8.utoronto.ca/ict/2021-annex_1-framework-standards.html).
[3] HM Government, "Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy," 2021.
[4] Sheng Jiang, "New IP Networking for Network 2030," Fifth ITU Workshop on Network 2030, International Telecommunication Union, October 15, 2019 www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf.

standards innovation.'[5] By leading standardization processes, China is looking to reshape the architecture of the Internet and set the rules that will govern the technologies of the future.

Standards setting also affords China the opportunity to build its own ideological tenets into the design and architecture of new tech. Just as the development of the Internet was shaped by the social values of engineers, governments and companies from the West,[6] China's New IP has an authoritarian flair. It is designed to capture large amounts of data and enable centralized controls that could be harnessed for government surveillance. Regardless of whether New IP succeeds in becoming standardized or being adopted at scale, it illustrates how the standardization of technologies that are not rights-respecting can legitimize their use, garner the protection of international trade rules, and challenge existing human rights norms.

This chapter will look at the standards journey and design features of New IP as a case study to illustrate how the development of technical standards is increasingly having ethical and human rights implications. The analysis of New IP will build on available evidence and depictions of its building-block technologies to infer how these alternative networking architectures may be used to enable surveillance and network controls. The chapter will also contribute to the existing body of scholarship on New IP by providing analysis on how this alternative networking model would result in domestic violations of human rights. Whether implemented by China within its territory or deployed by third countries, the text will outline how New IP would interfere with the right to privacy, freedom of expression and opinion, freedom of association and assembly of network users. In the specific case of China, the chapter will also argue that New IP could strengthen social control programs which make implementation of some human rights conditional on good behaviour, directly contrary to the principle of universality of human rights. Lastly, the text will conclude with a series of recommendations for human rights organizations, the technical community and governments to incorporate human rights into technology standardization processes and protect the global and open nature of the Internet.

2. Push to Standardize a New Internet Architecture

New IP is an attempt to build an alternative Internet. The proposal, first unveiled by Huawei in 2018 at ITU, puts forth a new model for connecting devices and sharing information and resources across networks.[7] Advocacy for New IP leverages two central Western policy

[5] China Electronics Standardization Institute, "Original CSET Translation of 'Artificial Intelligence Standardization White Paper,' Center for Security and Emerging Technology, Georgetown University, May 12, 2020 (https://cset.georgetown.edu/research/artificial-intelligence-standardization-white-paper/).
[6] Stacie Hoffmann, Samantha Bradshaw and Emily Taylor, "Networks and Geopolitics: How great power rivalries infected 5G," Oxford Information Labs, 2019.
[7] Initially referred to as "Decentralized Internet Infrastructure." See "Decentralized Internet Infrastructure (DII)," Light Reading (video), November 20, 2018. www.lightreading.com/blockchain/decentralized-Internet-infrastructure-(dii)/v/d-id/747708. The technology was introduced as 'New IP' at the ITU-T Telecommunication Standardization Advisory Group (TSAG) in 2019. See Huawei 2019, "New IP: Shaping the Future Network." Presented at the ITU-T TSAG, Geneva, Switzerland, September. https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2019-09-30-itu- t-tsag-ietf-iab-ls-on-new-ip-shaping-future-network-attachment-3.pptx.

concerns -- Internet security and growing control over Internet infrastructure and applications by a few large technology companies-- and claims to solve them through the application of decentralized technologies and the heightened use of identification methods for establishing trust on the network. In practice, this alternative Internet infrastructure would introduce new controls at the level of the network connection and enable bulk data collection and the option to track users and contents through the use of blockchain and permanent identifiers. These features can render New IP into an instrument for social control and state surveillance.

New IP can be described as an upgrade from the Great Firewall. Controls over online content in China have relied heavily on interventions at the level of Internet architecture. The Great Firewall, however, has been a patchwork solution to rein in the Internet. The upgrade of network controls through the creation of New IP would enhance digital contention already practiced in China.[8] Under New IP, data collection and control mechanisms would become more sophisticated as they would be built into the network architecture itself. New IP would streamline and feed in additional data into existing social monitoring initiatives such as the Social Credit System --a profiling program designed to influence behaviour that scores individuals based on their compliance with specific social norms -- and Chinese surveillance programs. This alternative version of the Internet designed to enable greater controls and surveillance would lend itself to human rights abuse.

Ongoing efforts to standardize New IP are a sobering example of the potential impact of technical standards on human rights, and in this specific case, on the future of Internet governance. New IP has the potential to fragment the global, open Internet, creating a parallel architecture that enables centralized government control. Depictions of the technology indicate that this parallel architecture would not be fully interoperable and therefore, in a best case scenario, potentially break the Internet into two large splinters. The splintering of the Internet is not an issue of competing engineering views on how the Internet should be structured. The emergence of New IP would fundamentally challenge core values and norms of open societies. This fragmentation would both contribute to and reflect the changing international world order and its normative underpinnings.[9]

2. (a). ITU as a Home for Multilateral Standards Development

There is a wide variety of organizations developing technical standards. These are generally divided between those that follow a multilateral model where consensus is developed among national country delegations, and those with an open standards model where participation is pluralistic, voluntary, bottom-up and driven by industry and innovation needs.[10] In the case of

[8] Ying Miao, “Managing digital contention in China,” *Journal of Cyber Policy*, 5:2 (07 Apr 2020), 218-238.
[9] Nick Merrill and Konstantinos Komaitis, “The consequences of a fragmenting, less global Internet,” *Brookings,* December 17, 2020, www.brookings.edu/techstream/the-consequences-of-a-fragmenting-less-global-Internet/.
[10] Konstantinos Karachalios and Karen McCabe. “Standards, Innovation, and their Role in the Context of the World Trade Organization.” International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2014.

Internet standards, the open standards paradigm has been instrumental in driving the Internet's success. Within this paradigm, the industry-led, multistakeholder Internet Engineering Task Force (IETF) is widely regarded as the primary SDO for defining protocols.[11]

While the natural home for introducing any updates to Internet standards would be the IETF, China instead opted to push for New IP's parallel architecture within the ITU standardization unit (ITU-T). Unlike the IETF's open standardization model, the ITU-T follows a multilateral model where member-states are the only participants to have a final say on approving recommended standards --or casting a vote when there is no consensus. This choice is unsurprising. ITU's multilateral, state-centric diplomacy gives China and its international allies a better shot at setting standards than multistakeholder SDOs would.[12] While other stakeholders can take part in deliberations at the ITU-T, participation costs are onerous and subject to the approval of the member state of the applicant.[13] As a result, non-state participation in ITU study groups is dominated by the private sector members who can afford the hefty fees to become 'sector members.' Dissident voices, on the other hand, are unlikely to be represented. In the case of China, its national delegation is not only the largest, but it has also integrated representatives from Chinese technology and telecommunications companies that spearhead proposals and advance specific agenda items.[14] This participation model has led to human rights and consumer protections being widely overlooked within the ITU's standards development space.[15]

Standardizing at ITU also represents a means to secure international trade protections for new technologies, giving approved standards a market edge.[16] The World Trade Organization's Agreement on Technical Barriers to Trade (TBT) encourages member states to adopt existing international standards from multilateral SDOs such as ITU.[17] Members are then required to use

[11] Other relevant entities include: ICANN, the regional Internet registries,W3C and IEEE which lead the development of policies for name and numbering resources, web standards. and physical and data link layers standards respectively. Internet standards are also shaped by mobile industry associations, such as 3GPP and GSMA; and regional bodies such as ETSI.

[12] Stacie Hoffmann, Dominique Lazanski and Emily Taylor, "Standardising the Splinternet: how China's technical standards could fragment the Internet," *Journal of Cyber Policy*, 5:2 (August 2020) 239-264.

[13] International Telecommunications Union, "Terms and Conditions" 2021 (www.itu.int/en/myitu/Membership/Become-a-Member/Terms-and-Conditions).

[14] Stacie Hoffmann and others, *Standardising the Splinternet*, p. 246.

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

[16] As per WTO, 'technical regulations in accordance with relevant international standards are rebuttably presumed 'not to create an unnecessary obstacle to international trade.'' See World Trade Organization, "Technical Information on Technical barriers to trade" n.d. (www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm).

[17] See World Trade Organization, "Technical Information on Technical barriers to trade" n.d, Article 2.4. The TBT considers as "international standards" those standards developed by organizations such as the ITU, International Standardization Organization (ISO), the International Electrotechnical Commission (IEC). See Konstantinos Karachalios and Karen McCabe. "Standards, Innovation, and their Role in the Context of the World Trade Organization." International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2014.

these standards to prove product compliance with WTO regulations.[18] In other words, ITU recommended standards become the gold standard for the import and export of technology. For China, standardizing at the ITU legitimizes the deployment of technologies domestically and, perhaps more importantly, it provides the country with a green card to export them.[19] WTO rules also prioritise adopted standards without consideration of human rights. While the TBT contemplates exceptions to the application of established standards, potential threats to human rights are not listed as a reason for departing from those standards. In this way, the international adoption of standards is unconcerned with human rights, yet protected by trade rules.

Although a detailed discussion of the role and mandates of other standards bodies is beyond the scope of this chapter, apart form IETF and ITU, there are several organisations active in the technical standards landscape, such as the International Standards Organisation (ISO) which is made up of a membership of 160 national standards bodies (such as the British Standards Organisation) (see figure 1). Like ITU, the ISO's standards are protected under WTO rules. There are also several industry-led standards bodies such as the Institute of Electrical and Electronics Engineers (IEEE) and the World Wide Web Consortium (W3C), all of which play a prominent role in standardising emerging technologies with a wide societal impact.

Chinese proposals have come at a time where ITU is looking to increasingly move beyond its original mandate, expanding from telecommunications into Internet standards and policy development. This unfolding trend has opened the door for New IP and its related technologies to be discussed within multiple ITU-T Study Groups (SGs) veiled under related applications or technologies such as blockchain, AI, and holographic communications.[20] The attempt to shift Internet standards development to the ITU risks transforming this dimension of Internet governance from a multistakeholder effort into a multilateral process.

[18] See World Trade Organization, "Technical Information on Technical barriers to trade" n.d, TBT Article 5.4.
[19] Stacie Hoffmann and others, *Standardising the Splinternet,* p. 246.
[20] To date, New IP-related work at ITU has been raised in multiple Study Groups including those dealing with protocols and test specifications (SG11), future networks and cloud (SG13), multimedia (SG16), security (SG17), and IoT and smart cities (SG20) (Stacie Hoffmann and others, *Standardising the Splinternet* p. 264).

Figure 1. Ecosystem of Technology Standards Development Organizations[21]

	Multilateral SDOs	**Open Standards, Multistakeholder SDOs**
Internet Technologies	ITU (Internet's physical layer) Mobile Technologies: 3GPP	Open Standards: IETF, IEEE, W3C, IAB Policy Development: ICANN, RIRs, IANA. Mobile Technologies: GSMA
Other Technologies	ITU, ISO, IEC, 3GPP	IEEE, GSMA

2. (b) China: Tech Super Power and Exporter of Cybernorms

The development of New IP has not happened in isolation. China's intent to become a tech super power has led the country to invest heavily in smart and emerging technologies, including areas such as 5G, big data and cloud computing.[22] New IP's proposed architecture would synchronize with telecommunications and networking technologies currently being promoted by China. If successfully standardized --entirely or partially through its various building blocks--, it is likely to become an integral part of the Chinese suite of products for export.

While the economic incentives behind standards-setting efforts are clear, the internationalization of Chinese technology also represents a means to export Chinese cyber-norms.[23] New IP's potential as an instrument for social control and state surveillance can encourage the adoption of techno-authoritarian practices elsewhere. Through design choices, China also embeds alternative approaches to human rights in the technologies that are being standardized. Weak privacy protections, disregard for anonymity and tolerance for surveillance are normally the

[21] Listed organizations are: ITU (International Telecommunications Union,https://www.itu.int/en/ITU-T/Pages/default.aspx); ISO (International Organization for Standardization, https://www.iso.org/home.html), IEC (International Electrotechnical Commission, https://www.iec.ch/homepage), IETF (Internet Engineering Task Force, https://www.ietf.org/), IRTF (Internet Research Task Force, https://irtf.org/)IEEE (Institute of Electrical and Electronics Engineers, https://www.ieee.org/standards/index.html), W3C (World Wide Web Consortium, https://www.w3.org/), IAB (Internet Architecture Board, https://www.iab.org/), ICANN (Internet Corporation for Assigned Names and Numbers, https://www.icann.org/), RIRs (Regional Internet Registries congregated under the Number Resources Organizations, https://www.nro.net/about/rirs/), IANA (Internet Assigned Numbers Authority, https://www.iana.org/), GSMA (Global System for Mobile Communications Association, https://www.gsma.com/) and 3GPP (3rd Generation Partnership Project, https://www.3gpp.org/).
[22] Max J. Zenglein and Anna Holzmann, "Evolving Made in China 2025. China's industrial policy in the quest for global tech leadership," Mercator Institute for China Studies, 2019.
[23] The Economist, "The digital side of the Belt and Road Initiative is growing," February 6, 2020, www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing.

distinctive features. Exported cyber-norms also reflect Chinese approaches to Internet and tech governance. By mainstreaming technologies that bypassed multistakeholder scrutiny, China legitimizes and reinforces multilateral technology governance.

China's primary strategy to secure new markets has been the Belt and Road Initiative (BRI), where the export of technology and digital infrastructure has featured prominently. Sometimes referred to as the Digital Silk Road, the BRI has created concrete opportunities to internationalize standards built-in into Chinese technologies. If the technology becomes available for implementation, pitching New IP to BRI participant countries would be likely to follow. In countries where Chinese equipment is already installed, deployment of New IP may only require software updates.

Beyond BRI trade partners, natural adopters of Chinese tech include authoritarian regimes that are enticed by the potential for social control through use of Chinese products.[24] These include some countries in the Gulf, Latin America, and Africa. Other countries are either attracted by price or captured through aid. Beyond offering competitive prices, Chinese tech companies are known to underbid to secure key contracts and expand the adoption of its technology --normally with the help of state subsidies.[25] In other cases, lending schemes are leveraged to secure concessions, including agreements to purchase and deploy Chinese tech. Several BRI participating countries have already agreed to adopt Chinese technology for the deployment of 5G networks.[26] These strategies are affording China a growing role in developing countries where the country has sought to influence communications infrastructure plans for decades. Developing countries also host large segments of the 2.7 billion people that are yet to come online.[27] This represents a huge market potential that China is well positioned to conquer with its lower-priced technology.[28]

Through China's seizable domestic market of 1.43 billion people, the leverage over BRI partners and the commercial power of Huawei, New IP could well become a de-facto standard. In other words, domestic adoption and export of New IP do not necessarily hinge on international standardization. The clincher, however, lies in the legal protections and legitimation that Chinese technologies acquire once standardized. This has made China's pursuits within ITU increasingly central to the country's strategy for technology dominance.

---

[24] Stacie Hoffmann and others, *Standardising the Splinternet*, p. 254.
[25] Stuart Lau and Reuters, "EU seeks to curb investment by state-backed buyers from China and other countries," The South China Morning Post, June 17, 2020, https://www.scmp.com/news/world/europe/article/3089474/eu-wants-curb-company-takeovers-state-backed-buyers-china-other and Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, August 6, 2020, www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.
[26] Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, August 6, 2020, www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.
[27] Internet World Stats, https://www.Internetworldstats.com/stats.htm, accessed 10 July 2021.
[28] The Economist Special Report, "The digital side of the Belt and Road Initiative", *The Economist,* February 6, 2020, www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing.

2. (c). Where is New IP today?

Huawei publicly declared in September 2020 that New IP has already undergone gap analysis, conceptual research as well as testing, and that the idea was "solid, viable, and feasible in*[sic]* implementation.[29]" Company leadership also confirmed Huawei's intent to move ahead with the standardization of New IP within ITU.[30] China has even conducted a live demonstration of New IP at ITU as part of the controversial focus group *Network 2030* which was tasked with scoping technology needs for the future of networks.[31]

China's standards strategy --reflected both in China's Standards 2035 blueprint and most recent Five Year Plan-- suggests that deployment of New IP is likely to start domestically, while the country works to legitimize national standards internationally through ITU and other SDOs amenable to discuss Chinese standards.[32] Large scale piloting appears to have started in April 2021, with the announcement of a backbone network that will connect 40 leading universities to test what has been advertised as the 'Internet of the Future.'[33] This test bed exercise is expected to verify the performance and security of the network prior to commercial deployment. With its sizable domestic market, China's government could achieve a scale deployment of New IP at home. Domestic deployments alone would serve to get New IP pass proof of concept, improving its chances of uptake elsewhere.

In 2020, as red flags were raised around China's efforts to standardize New IP, multiple country delegations and sector organizations voiced their concerns at ITU-T, including the UK, Norway, 21 EU member states, the European Commission, the Regional Internet Address Registry RIPE

[29] "'New IP' and Global Internet Governance," Georgia Institute of Technology, Internet Governance Project and Internet Society (video), September 23, 2020 (www.Internetsociety.org/events/new-ip-and-global-Internet-governance/).
[30] "'New IP' and Global Internet Governance," Georgia Institute of Technology, Internet Governance Project and Internet Society (video), September 23, 2020.
[31] ITU-T, "Technical Report: Network 2030 - Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020" June 2020, (www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Description_of_Demonstrations.pdf?csf=1&e=D7M69p).
[32] Alexander Chipman Koty, "What is the China Standards 2035 Plan and How Will it Impact Emerging Industries?" July 2, 2020 (www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/) and Xinhua News Agency, "Original CSET Translation of 'Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035,' Center for Security and Emerging Technology, Georgetown University, May 13, 2020 (https://cset.georgetown.edu/publication/china-14th-five-year-plan/).
[33] Stephen Chen, "China starts large-scale testing of its Internet of the future," *South China Morning Post,* April 20, 2021, www.scmp.com/news/china/science/article/3130338/china-starts-large-scale-testing-its-Internet-future.

NCC, the IEEE, and IETF itself.[34] Leading associations within the telecommunications industry have also spoken against New IP, indicating that the sector does not support the proposal.[35]

While this signals that Western organizations are taking notice, Chinese efforts are unlikely to relent. Following the rejection of the original New IP proposal within ITU, Chinese delegations have emerged with a new strategy: standardizing New IP in pieces. This has manifested in proposals to kickstart the standardization process of New IP's building blocks technologies such as the use of blockchain to modify the nature of identification systems used on the Internet, or the transformation of networking protocols to incorporate identifiers and expose information from data packets traveling on the net.[36] The new approach of breaking the proposal into smaller building blocks, accompanied with more specific examples of practical, industrial uses of the technology, addresses a key criticism of the original New IP: the lack of compelling use cases. This makes it less likely that the new proposals could simply be dismissed out of hand within the standards development environment. Despite the new presentation, if put together, New IP's building blocks could still deliver a parallel Internet with unmatched surveillance capabilities.

As part of its efforts to influence standards, China has also resorted to forum shopping. The China Internet Network Information Center, for instance, has filed a US patent application (published 6 May 2021) for decentralized blockchain DNS.[37] China's recent 14th Five-Year Plan released in March 2021 indicates that intentions to embed blockchain technologies into Internet architecture for enhanced centralization and tracking, as well as to step up the social credit system, are still firm objectives of the Chinese Communist Party (CCP).[38]

Similarly, Russia is challenging the existing procedures to manage the Internet globally. In January 2021, Russia presented a proposal at ITU calling into question the status of the global

---

[34] See TSAG Contribution 135 entitled "Response to "New IP, Shaping Future Network" proposal" (RIPE NCC, January 28 2020), TSAG Contribution 139 entitled "New IP" (Austria and others, September 7, 2020), TSAG Contribution 156 (IEEE, September 8, 2020) and ITU-T TSAG Liaison Statement entitled "LS on New IP, Shaping Future Network" (IETF, March 20, 2020).

[35] These include the European Telecommunications Network Operators' Association (ETNO) and the Global System for Mobile Communications Association (GSMA). See ETNO, "ETNO position paper on the New IP proposal," November 5, 2020 (https://www.etno.eu/library/positionpapers/417-new-ip.html) and ITU-T SG13 Contribution 1069 entitled "New IP, Future Vertical Communication Networks or similar proposals" (Austria and others, November 18, 2020).

[36] See for example: recommendation entitled "Scenarios and requirements of network resource sharing based on distributed ledger technology" presented by China Telecom, China Unicom, ZTE, Huawei scheduled for Q4 2022; recommendation entitled "Scenarios and Requirements of Intent-Based Network for network evolution" presented by China Telecom and the Ministry of Industry and Information Technology of China scheduled for Q4 2022; and IETF submission entitled "Gap Analysis in Internet Addressing," July 12 2021.

[37] Andrew Allemann, "China wants to patent a decentralized blockchain DNS," *Domain Name Wire,* May 10, 2021https://domainnamewire.com/2021/05/10/china-wants-to-patent-a-decentralized-blockchain-dns/.

[38] Xinhua News Agency, "Original CSET Translation of 'Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035,' Center for Security and Emerging Technology, Georgetown University, May 13, 2020 (https://cset.georgetown.edu/publication/china-14th-five-year-plan/).

governance system for Internet domain names, addresses, and critical Internet infrastructure.[39] The Russian request did not stick, and the specific New IP proposals may not eventually be standardized, but both examples speak to China and Russia's joint and separate determination to challenge the Internet's governance model.

The World Telecommunication Standardization Assembly (WTSA) 2020 was postponed due to the pandemic and is currently scheduled to take place in March 2022. WTSA will reveal whether China and its allies have been able to build sufficient consensus to move New IP proposals --or reconfiguration of its building block technologies-- ahead. Whatever the outcome from WTSA, China is likely to continue reinforcing narratives around decentralization and trust which draw on legitimate policy concerns from the West to justify New IP, perhaps across other standards bodies or international fora.[40]

3. Human Rights Implications of New IP

Huawei has presented the development of New IP as a purely technical proposal to evolve the network layer of the Internet stack --the suite of communication protocols that make up the Internet. It has also defended its attempt to standardize Internet technologies outside of multistakeholder SDOs, alleging that organizations that have successfully contributed to the growth of the Internet such as the IETF are 'too slow to keep up with innovation.'[41] While technology development and standardization may be expressed as merely an engineering exercise, New IP and its supporting technologies would have a significant impact on fundamental human rights.

3. a. Understanding How New IP Enables Surveillance

At its core, New IP would render the Internet an instrument for government control. From a technical standpoint, what New IP proposes is a restructuring of the Internet architecture that modifies how the various Internet layers operate (see figure 2). The Internet's original design foresees a model where layers operate independently and largely unaware of one another. This design has enabled the speed and affordability which has made the Internet the success it is. Under New IP, the main change is that the network layer --how information packets travel-- would be transformed by incorporating new capabilities that grant those entities involved in managing networks and nodes greater control over Internet traffic and users.

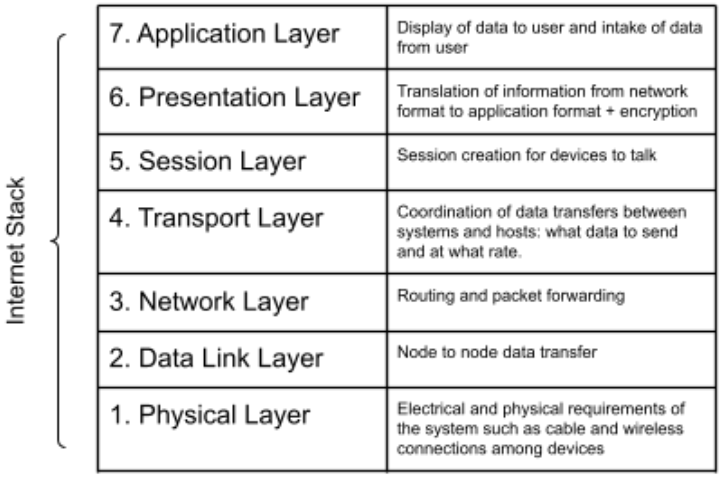
---

[39] David Ignatius, "Russia is trying to set the rules for the Internet. The U.N. saw through the ruse," *Washington Post,* February 1, 2021 www.washingtonpost.com/opinions/2021/02/01/russia-Internet-rules-united-nations/.

[40] For discussion on Chinese narratives on decentralization and 'decentralized trust,' see Stacie Hoffmann and others, *Standardising the Splinternet*, p. 249-50.

[41] "'New IP' and Global Internet Governance," Georgia Institute of Technology, Internet Governance Project and Internet Society (video), September 23, 2020.

Figure 2. Internet Layers - Open Systems Interconnection (OSI) Model[42]



The network layer is often referred to as “the dumb pipes" of the Internet, as it is tasked with the transport of data packets, while unconcerned about the content of those packets. This simplicity in design was adopted intentionally to keep Internet standards lightweight and interoperable.[43] Traditionally, a line was drawn between the application layer and the core architectural layers. The application layer is the interface between humans and technology, where communications become visible and where content is created and consumed by people. The application layer is inherently political: it is where the human rights of freedom of expression, privacy, freedom of thought and opinion are most obvious. The core architectural layers on the other hand offer the means for transporting information and constitute what could be described as the neutral foundations of the Internet.

Chinese delegates proposing New IP claim that the dumb network layer is inadequate for the deployment of future technologies such as holograms and self-driving cars that will require very low latency --meaning minimal delays when processing high volumes of data-- and guaranteed data delivery.[44] While it is unclear whether New IP could truly deliver on those promises,[45]- the proposed enhancement of the network layer would render networking a new locus for control.

Under New IP, the network layer would become more complex. Specifically, New IP proposes to embed information from the application layer into the no longer ‘dumb pipes’ of the network

[42] Keith Shaw, “The OSI model explained and how to easily remember its 7 layers,” *Networkworld*, October 14, 2020, www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html.
[43] See, for example, IETF RFC 1958 entitled “ Architectural Principles of the Internet” (June 1996).
[44] Anna Gross and Madhumita Murgia, “China and Huawei propose reinvention of the Internet,” *Financial Times*, March 27, 2020, www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2; and Jon Fingas, “China, Huawei propose Internet protocol with a built-in killswitch,” *Engadget,* March 30, 2020, /www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.
[45] Marco Hogewoning, “Do We Need a New IP?,” *RIPE NCC*, 22 April 2020, https://labs.ripe.net/author/marco_hogewoning/do-we-need-a-new-ip/.

layer.[46] This would generate a degree of vertical integration that undermines the principle of layer independence that characterizes the Internet's original design. Under this new networking model, the packet header --the outside of a box that establishes where a packet is headed-- would be modified to also include a description of the contents (see figure 3). With this information so readily available, the upgraded, intelligent network layer would become a proxy for control, and policy issues previously reserved to the application layer would move down the Internet stack.[47] Infrastructure providers that supply networking equipment such as routers, and Internet Service Providers (ISPs) that operate the networks, would become key players in managing 'services, access controls, and application of policy and regulation that would now take place at the point of connection.'[48]

Beyond transforming the networking layer, New IP also sets out to reconceptualize the unique identifier systems that underpin the Internet.[49] This is done through the incorporation of immutable identifiers and "burned in" addresses throughout the networking process and the introduction of Decentralized Ledger Technologies (DLT) --more commonly known as blockchain-- into the networking architecture. These technologies would significantly alter the nature of the Internet introducing new tracking capabilities, facilitating access to data and information controls, and also undermining the governance models of current Internet identifiers such as domain names and addresses.

Identifiers are used to locate and retrieve information by assigning unique, permanent names to 'things' on the Internet (such as users, content, routers, servers, devices). Within New IP proposals, these identifiers have been described as bit strings that are centrally administered and immutable. The reliance on persistent, one-to-one relationships between an identifier and an object would enable unparalleled tracing over the Internet through the creation of permanent records, for example, on users' browsing history. Additionally, using these identifiers, the network could be instructed to discard packets or disconnect devices that are deemed illegitimate, through what New IP depictions describe as the "shut off" protocol.[50]

---

[46] Just as intelligence from the application layer is integrated into the networking layer, the network may signal information back to the application layer.

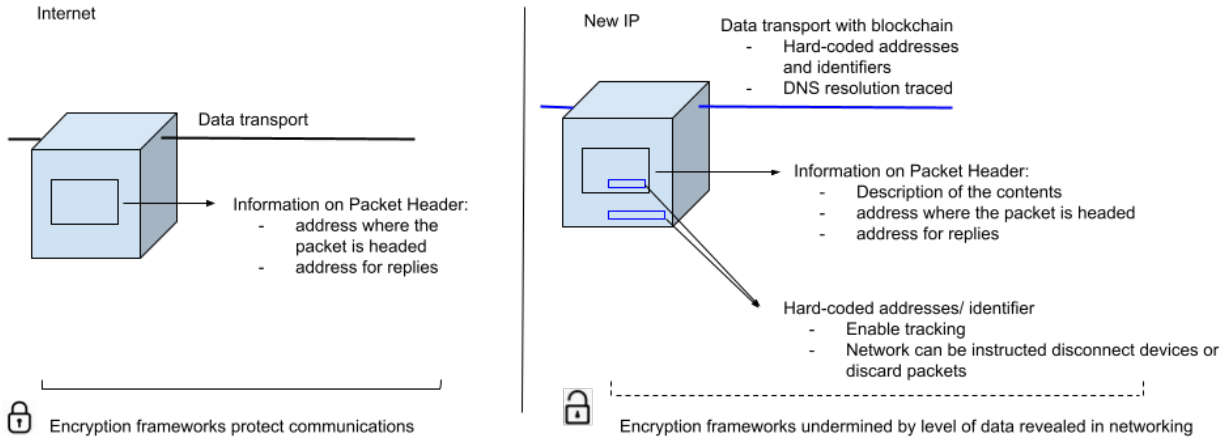
[47] There are other areas where standards are raising human rights concerns. DNS over HTTPS (DoH) and Transport Layer Security (TLS) 1.3 are two such examples. These standards seek to protect privacy and surveillance threats but can potentially generate unintended effects that weaken the stability and security of the Internet.

[48] Stacie Hoffmann and others, *Standardising the Splinternet*, p. 245.

[49] Unique identifiers include domain names, Internet Protocol addresses, Autonomous Systems Numbers and Port Numbers; these identifiers are central for current Internet protocols to function. See the Internet Corporation for Assigned Names and Numbers, "ICANN Acronyms and Terms," n.d. www.icann.org/en/icann-acronyms-and-terms/unique-identifier-en.

[50] Huawei 2019, "New IP: Shaping the Future Network." Presented at the ITU-T TSAG, Geneva, Switzerland, September. https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2019-09-30-itu- t-tsag-ietf-iab-ls-on-new-ip-shaping-future-network-attachment-3.pptx.

Figure 3. Internet and New IP networking models



Decentralized Ledger Technologies (DLTs) are also being proposed for standardization in ways that would transform the Internet's existing identifiers systems, primarily the Domain Name System (DNS).[51] Huawei's descriptions of New IP include a blockchain layer which would operate at the point of networking connection to provide what Huawei representatives have described as the "decentralized trustworthiness of the Internet name spaces.[52]" This claims to solve DNS security issues through the verification of IP address ownership and tracking of DNS resolution. Presented as a security feature, in practice, this allows unparalleled tracing over the Internet.

DLT's distributed nature and reliance on encryption means the technology is normally associated with being decentralized and secure. However, these features are dependent on how the technologies are implemented. Applied to the Internet architecture as proposed within New IP, DLT would generate opposite effects.[53] The use of DLT would allow for centralized control, streamline data collection and further facilitate individualized tracking of users and content. DLT also automatically collects and shares data with designated entities.[54] This means it could be employed by governments to share, gather, aggregate and analyze data. These features are likely to be supported and further enhanced by 5G's edge computing.[55]

---

[51] Chinese delegations are already working through ITU to standardize the use of DLT in Internet architecture. Chinese companies first submitted Contribution 693 at SG 13 in 2019 to discuss the creation of a decentralized DNS root based on blockchain. As per SG13's work program, conversations on DLTs are set to continue throughout the 2021-2022 period. See for example recommendation entitled "Framework and Requirements of Decentralized Trustworthy Network Infrastructure" scheduled for Q3 2021.

[52] "Decentralized Internet Infrastructure (DII)," Light Reading (video), November 20, 2018. www.lightreading.com/blockchain/decentralized-Internet-infrastructure-(dii)/v/d-id/747708.

[53] One main feature of DLTs is that transactions are immutable. From a security perspective, replacing the DNS with blockchain means that threats such as fraud become almost permanent as they are hard, if not impossible to undo.

[54] Stacie Hoffmann and others, *Standardising the Splinternet*, p. 250.

[55] Stacie Hoffmann and others, *Standardising the Splinternet*, p. 244.

Lastly, the secured implementation of this technology depends largely on who controls the DLT. In China, state owned entities are likely to have control over the DLT and the data it processes; likewise, governments that import these technologies could facilitate similar arrangements. Combined with immutable identifiers as described in some New IP proposals, every action and transaction becomes traceable and allows for surveillance and scrutiny. This would further erode anonymity online and open the door to mass surveillance. In other words, the distributed nature of DLT does not prevent centralization, and the mere use of blockchain encryption does guarantee privacy or protection from surveillance. There are a number of additional concerns about the integration of blockchain into a large-scale network such as its high power consumption and environmental impact, and the latency on routing decisions which would erode the user experience. These considerations, though valid, are beyond the scope of this chapter.

3. b. How New IP is not Human Rights Respecting

The capture, transfer and use of personal data envisioned by New IP would violate states' obligations in the International Bill of Rights[56] to respect and ensure human rights,[57] and corporate actors' responsibilities, reflected in the UN Guiding Principles on Business and Human Rights, to respect human rights in their activities.

New IP would be significantly more intrusive than current forms of online surveillance. Under this model, surveillance would not happen through hacking or interfering with the network. Instead, New IP would build surveillance capabilities into the Internet architecture itself. If adopted, New IP's data gathering, individual tracking, and users and content control capabilities would threaten multiple human rights. This section will discuss the impact that a New IP network model would have on the right to privacy and other human rights that are essential for the health of open and free societies. The section will also address how New IP would contribute to China's social control and surveillance ecosystem, and undermine the principle of universality of human rights by facilitating systems where access to rights is contingent on the fulfillment of responsibilities.

New IP would place surveillance data both in the hands of corporate actors - ISPs and infrastructure providers - and the governments with which they collaborate. In the case of China, the companies that would hold the information yielded by New IP are either government-controlled or have close links with the government.[58] It is commonplace in China for the government to capture and use private sector-generated data. Data-sharing requirements

[56]The Universal Declaration of Human Rights (UDHR), International Covenant on Economic, Social and Cultural Rights (ICESCR) and International Covenant on Civil and Political Rights (ICCPR). China is not a party to ICCPR but arguably many of its obligations reflect customary international law. China is a party to ICESCR.

[57] As per ICCPR Article 2 (1), States are required to respect and ensure the rights recognized in the Covenant, including the right to privacy.

[58] For instance, there are few Chinese ISPs and they are all state-owned: China Unicom, China Telecom, and China Mobile.

between the government and private sector are often built into local regulations and are likely to be broadened in the years to come.[59]

3. b. i. Impacts on Privacy

The right to privacy is protected in Article 12 of the Universal Declaration of Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR) as well as regional human rights treaties. At its heart, this right seeks to defend individuals' private sphere --an area for autonomous development, interaction and liberty that is free from State intervention.[60] The right to privacy includes informational privacy --that is, privacy in information that exists, or that can be deduced, about a person. This includes information from online communications and metadata.

While technology-mediated, mass data collection by both private and public actors is increasingly common, it must not unduly interfere with privacy. International human rights law and standards set out clear rules on the circumstances under which interferences with the right to privacy are permissible. In broad terms, any interference must be provided for by clear and publicly accessible law, pursue an objectively legitimate aim, and be necessary and proportionate to achieving that aim.

The precise parameters of acceptable interferences with the right to privacy in the collation, retention and use of online data are being discussed in parallel with ongoing developments in information-gathering technologies and artificial intelligence. David Kaye, during his appointment as UN Special Rapporteur on freedom of opinion and expression, called for an immediate moratorium on the global trade and use of surveillance technologies until 'rigorous human rights safeguards are put in place to regulate such practices.'[61] The statement was made with reference only to targeted surveillance. When considering mass surveillance, the challenge becomes even more severe and begs the question whether safeguards can ever be robust enough to mitigate such risk. The European Union's proposed regulation on Artificial Intelligence is one example of an effort to develop a legal framework which ensures respect for human rights, including through the creation of robust safeguards that would mitigate potential threats to rights from mass surveillance.

Wherever the parameters of acceptable mass collection of data and surveillance lie, it is clear that New IP would fall far short of compliance with the right to privacy.

---

[59] Upcoming updates to cybersecurity regulations, namely the Multi-Level Protection Scheme 2.0 and the Cryptography Law, are expected to require companies that hold sensitive data to undergo "cybersecurity monitoring" connected to the public security agency and to adopt Chinese algorithms for encryption. See Samm Sacks, "Data Security and U.S.-China Tech Entanglement," *Lawfare,* April 2, 2020, www.lawfareblog.com/data-security-and-us-china-tech-entanglement.

[60] United Nations Human Rights Council, "The Right to Privacy in the digital age. Report of the United Nations High Commissioner for Human Rights," UN doc A/HRC/39/29, 3 August 2018.

[61] United Nations Human Rights Council, "Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," UN doc A/HRC/41/35, 28 May 2019.

Both case law and commentary from international organisations relate to privacy infringements far less intrusive than that enabled by New IP. From them, it is clear that New IP would violate the right to privacy in four distinctive ways.

Data collection: The right to privacy entails that any collection of personal data must be fair, lawful and transparent.[62] Laws permitting the collection of personal data must guarantee that data can only be accessed by those who need it, ensure that it is only processed for purposes compatible with international human rights law, and enable individuals to ascertain what data is held about them, and by whom. Laws should also enable individuals to request the correction and deletion of that data. In practice, many states have sought to translate these requirements through data protection laws, such as the General Data Protection Regulation in the European Union.

Much debate has taken place about whether 'bulk' data collection constitutes an act of surveillance. Recent analysis by the United Nations High Commissioner for Human Rights indicates that data collection relating to 'a person's identity, family or life' interferes with the right to privacy.[63] Data does not need to be examined by a person or an algorithm for privacy to be impacted; the mere collection of information means that 'an individual loses some control over information that could put his or her privacy at risk.'[64] The Court of Human Rights (ECtHR) too has reinforced these standards in its recent Big Brother Watch decision which set a new precedent against indiscriminate data collection for Council of Europe (CoE) member states.[65]

New IP would not meet privacy standards on data collection. Its reliance on DLT would allow the gathering of data such as browsing history and online habits and, through immutable identifiers, that data could be attributed to specific users or devices. In addition, any metadata collected through the deployment of DLT that when aggregated could give an insight into an individual's 'behaviour, social relationships, private preferences and identity'[66]- would too constitute an interference with violation of the right to privacy.

---

[62] United Nations Human Rights Council, "The Right to Privacy in the digital age," UN doc A/HRC/39/29, 3 August 2018, para 29.
[63] United Nations Human Rights Council, "The Right to Privacy in the digital age" UN doc A/HRC/39/29, 3 August 2018.
[64] United Nations Human Rights Council, "The Right to Privacy in the digital age." UN doc A/HRC/39/29, 3 August 2018; and United Nations Human Rights Council, "The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights," UN doc A/HRC/27/37, 30 June 2014.
[65] ECtHR ruled that the UK government's bulk data collection practices revealed by Edward Snowden in 2013 breached citizens' right to privacy. See Big Brother Watch Team, "UK mass surveillance found unlawful by Europe's highest human rights court," Big Brother Watch, May 25, 2021, https://bigbrotherwatch.org.uk/2021/05/uk-mass-surveillance-found-unlawful-by-europes-highest-human-rights-court/.
[66] United Nations Human Rights Council, "Resolution 42/15," UN doc A/HRC/RES/42/15, 26 September 2019.

Surveillance: Surveillance is only permissible if --in addition to the general requirements relating to interferences with the right to privacy-- it is limited in scope and duration, targeted and subject to independent authorization and oversight.[67] According to UN Human Rights Council (HRC) Resolution 42/15, arbitrary surveillance, interception of communications and collection of personal data are all violations or abuses of the right to privacy.[68] Similarly, in the context of the COVID-19 pandemic, HRC Resolution 47/23 of July 2021 highlights how response measures to the pandemic have 'reinforced the need to address arbitrary surveillance not in accordance with States' obligations under international human rights law and inconsistent with the principles of necessity, proportionality and legality'.[69]

New IP would not meet privacy standards on surveillance. Its alternative networking model would enable mass surveillance at an unprecedented scale. Merics reports that China has rolled out surveillance initiatives such as Golden Shield, Skynet, Safe Cities and Police Clouds, and Project Sharp Eyes, yet these currently face challenges of lack of digitization and harmonization across states.[70] New IP would have the capacity to offer streamlined access to data and profiling mechanisms for the benefit of such surveillance programs. Even if, as some liberal democracies argue, some mass surveillance can be justified on the basis of national security, New IP goes far beyond being a proportionate response to any conceivable threat. It would enable mass scale, long term monitoring of the population in all circumstances, clearly not compatible with the right to privacy.

Erosion of anonymity: As assessed by the former UN Special Rapporteur on freedom of expression, anonymity online is necessary for the exercise of the right to freedom of opinion and expression, and any restrictions on it must be strictly limited to measures that are lawful, necessary, proportionate and in furtherance of a legitimate objective.[71]

The erosion of anonymity contemplated by New IP would meet none of these conditions. New IP would undermine anonymity by weakening encryption frameworks used in the Internet. The proposed reconfiguration of the networking layer would expose a great deal of information on users and contents. With this information so readily available, the ability of existing encryption efforts to prevent content inspection and censorship would be severely curtailed. Using burned-in identifiers, no longer anonymous users could be effectively blocked off the network. Unprotected communications would also be exposed to inspection and content blocking.

New IP would also co-opt existing trust mechanisms, such as blockchain encryption, and incorporate them into its surveillance architecture. New IP proponents maintain that blockchain

[67] United Nations Human Rights Council, "The Right to Privacy in the digital age," UN doc A/HRC/39/29, 3 August 2018.
[68] United Nations Human Rights Council, "Resolution 42/15. The right to privacy in the digital age" UN doc A/HRC/RES/42/15, 26 September 2019.
[69] United Nations Human Rights Council, "New and emerging digital technologies and human rights." UN doc A/HRC/47/L.12/Rev.1, 13 July 2021.
[70] Katja Drinhausen and Vincent Brussee, "China's Social Credit System in 2021," p.19.
[71] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 22 May 2015 (A/HRC/29/32). See paragraph 56.

and DLTs will render the network safe. However, as conceived under New IP, DLTs actually place great control on whoever manages its implementation --likely, government authorities or state-owned operators.[72] The erosion of mechanisms that help protect anonymity could have a significant negative impact on dissidents, human rights defenders, journalists and activists who rely on these tools to communicate freely.[73] It would also jeopardize all Internet users by rendering them vulnerable to state interference.

Permanent user profiles: New IP could enable the creation of permanent profiles on individuals. The adoption of permanent user profiles would amount to a gross violation of the right to privacy and have a chilling effect on other rights. New IP's combined use of DLT and identifiers would enable the creation of permanent profiles on individuals recording their online activity on ledgers. This level of individualized tracking offered by New IP would threaten anonymity online, if not eliminate it as a whole. It would potentially feed private activities online into social control or surveillance programs, such as China's social credit system, by which financial credit and other social advantages are being made contingent on socially acceptable behaviour, and the Golden Shield Project (the "Great Firewall"), by which accessible Internet content is controlled.

The interest in applying DLT for tracing individuals is not new for Chinese authorities. In 2018, the Chinese Central Internet regulator proposed legislation to require blockchain companies to sign up users using their national ID numbers.[74]

Comparison with Western data collection and surveillance practices

Mass surveillance is certainly not unknown in the West. The Edward Snowden revelations uncovered unlawful practices of domestic and foreign surveillance emerging from the United States.[75] The amount of data amassed and used by social media and tech companies too is increasingly perceived as infringing on privacy.[76] While the mass surveillance undertaken by Western governments is arguably disproportionate, New IP and related social control would embody different surveillance objectives --control of behaviour, rather than for an aim recognised by international human rights law as legitimate such as national security or the prevention of crime. Surveillance under New IP would also happen at a wholly different scale, being the norm rather than the exception whenever the Internet is used. Moreover, being all-

[72] Stacie Hoffmann and others, Standardising the Splinternet, p. 250.
[73] United Nations Human Rights Council, "The Right to Privacy in the digital age." UN doc A/HRC/39/29, 3 August 2018. See paragraph 20.
[74] Zheping Huang, "China requires blockchain-based information service providers to register users using real names, censor postings and store user data," South China Morning Post, October 22, 2018, www.scmp.com/tech/blockchain/article/2169613/china-requires-blockchain-based-information-service-providers; and Article 19, "Blockchain: Technology alone cannot protect freedom of expression," July 01, 2019, www.article19.org/resources/blockchain-technology-alone-cannot-protect-freedom-of-expression/.
[75] Raphael Satter "U.S. court: Mass surveillance program exposed by Snowden was illegal," *Reuters,* September 2, 2020, www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK.
[76] Bennett Cyphers and Cory Doctorow. "Privacy Without Monopoly: Data Protection and Interoperability," Electronic Frontier Foundation, 2021.

pervasive and invisible, there would be no checks and balances to restrain the impact of New IP and related measures, such as transparent rules with the opportunity to seek redress for breach through the courts; opportunities to highlight and protest against poor practice publicly and in the media; and the potential for investor scruple that restricts investment in rights-violating systems.

3. (b). ii. Impact on other rights that enable open and free societies

New IP's surveillance capabilities would not only have an impact on individuals' right to privacy, but would also interfere with other civil and political rights that are essential for democratic societies. These include the right to freedom of opinion and expression and right to freedom of peaceful assembly and association. As with the right to privacy, international human rights law is clear that any restrictions on these rights must be provided for by clear and publicly accessible law, pursue an objectively legitimate aim, and be necessary and proportionate to achieving that aim.

New IP would impact freedom of opinion and expression in multiple ways. First, data gathering and surveillance can lead to self-censorship.[77] New IP would exert an overt form of surveillance, as network users would likely be aware of the possibility of individualized tracking of online activity. This would set off a Panopticon effect, meaning that New IP users may adjust their online behaviour, and particularly their communications and the information they search for and share, knowing they may be observed.[78] Second, if users know that its surveillance mechanisms may be used to impose consequences such as access to social credit, New IP could serve as a mechanism to silence dissent and enforce control. Lastly, New IP could interfere with users' ability to seek, receive and impart information and to inform opinions without interference. Specifically, entities in charge of managing DLT could block both users or content.

Similarly, New IP could have chilling effects on the right to freedom of peaceful assembly and association. New IP could be leveraged by governments to disable online channels to organize by blocking: (a) specific users, such as dissidents or perceived troublemakers; (b) specific sites and platforms that bring together protestors; or (c) specific content related to the purpose of mobilization. These actions could be interpreted as micro-targeted shutdowns, which would in turn help governments avoid unpopular, complete network shutdowns that are commonplace today. These types of interference would undermine the right of assembly by essentially restricting the ability to effectively mobilize.[79] Similarly, New IP would enhance the ability of governments to surveil protestors, either through mass surveillance mechanisms enabled by data collection or targeted surveillance enabled by user profiles. In this case, freedom of

[77] United Nations Human Rights Council, "Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," UN doc A/HRC/44/24, 28 May 2019.
[78] Paul Bernal "Data gathering, surveillance and human rights: recasting the debate," *Journal of Cyber Policy*, 1:2, (September 16, 2016) 243-264.
[79] United Nations Human Rights Council, "Surveillance and human rights." 28 May 2019.

peaceful assembly and association would be impacted as the result of New IP's undermining of encryption and anonymity.

3. (b). iii Discrimination

Article 2.1 ICCPR requires States not to discriminate in their implementation of rights, and Article 26 entitles all persons to equality before the law and protection against discrimination on any ground. Similarly, Article 2.2 of International Covenant on Economic, Social and Cultural Rights (ICESCR) requires State to implement economic, social and cultural rights without discrimination.

The enhanced individualized tracking and profiling enabled by New IP would facilitate the discriminatory treatment of individuals and groups. For example, individualized tracking through New IP may place minorities at risk. States would have the tools to single out target groups, track their online activity, persecute them or coerce them into adopting desired behaviours. China's well documented surveillance of the Uighurs through the Joint-Operations Platform (IJOP) in Xinjiang indicates that these potential uses are not far-fetched. These efforts would run in parallel with other efforts to reinforce discriminatory practices through technology such as in AI, with several Chinese firms filing patents and seeking to standardise facial recognition software that claims to be able to identify religious or ethnic minorities by their features.[80]

3. (b). iv. Risks of Conditional Implementation of Human Rights

New IP would enable the creation of data logs and collection of information at an unprecedented scale. If deployed domestically within China, government agencies in charge of managing New IP's blockchain logs could easily share collected data to implement or strengthen profiling, scoring and ranking mechanisms that render access to rights and benefits conditional on meeting specific criteria: in other words, to make human rights implementation contingent on meeting conditions or responsibilities. Such mechanisms seek to penalize and impose consequences on those monitored. Social benefits and freedoms such as freedom of movement may be denied as a form of punishment in order to control behavior. Such consequences could be imposed not only on groups linked by a characteristic (discrimination) but also on individuals by reference to their behaviour.

This is seen through China's social credit system. The building of a social credit system, first formalized as a national objective in 2014, is an ongoing development and still features as a priority in the country's most recent five year plan. At its heart, it is a reward and punishment mechanism designed to render entry into various market transactions contingent upon scoring of behaviour which applies to both individual and corporate actors. Unlike financial credit scoring systems in the West, the Chinese social credit system takes account of not only financial

[80] Leo Kelion, "Huawei patent mentions use of Uighur-spotting tech," BBC, January 13, 2021, www.bbc.co.uk/news/technology-55634388 and Anna Gross and others, "Chinese tech groups shaping UN facial recognition standard" Financial Times, December 1, 2019 www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

information, but also nonfinancial data such as travel, health and police data gathered from a multiplicity of agencies and sources.[81] The system operates not through the imposition of new obligations, but rather as a mechanism to strictly enforce existing regulations, including those that may lead to discriminatory treatment of individuals.[82]

Multiple reports indicate that China's social credit pursues primarily financial and commercial goals;[83] yet the system has eerie effects in the enjoyment of rights. China is reported to have banned citizens from buying plane or train tickets by the millions, and some local governments are also experimenting with additional limitations, barring low-performers from financial services and real estate.[84]

In practice, China's roll-out of social credit appears to have been challenging and far from uniform. There are diverse social credit regimes across various units of government with varying assessment criteria and scope.[85] The creation of separate systems across the country has resulted in a marked fragmentation.[86] In addition, social credit systems are not fully digitized, relying heavily on non-systematized data and human analysis.[87]

New IP would largely resolve these challenges of implementation, and facilitate further systems of contingent access to rights. New IP's reliance on DLT would facilitate nationwide data collection and data sharing with designated entities, such as government agencies and corporations that participate in social credit schemes.[88] The combined use of DLT and identifiers would further strengthen the creation of fully digital, permanent records on individuals. By significantly increasing the data-driven analytical power of the Chinese state, New IP would align very closely with China's data governance priorities to create a cohesive information ecosystem across regions and administrative levels.[89]

---

[81] Fan Liang and others, "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure," *Policy & Internet,* 10- 4, (2018) 415-453; and Democratic Staff Report, "The Big Brother: China's Digital Authoritarianism," Committee on Foreign Relations, United States Senate, July 21, 2020.

[82] Katja Drinhausen and Vincent Brussee, "China's Social Credit System in 2021" Mercator Institute for China Studies, March 2021.

[83] Fan Liang and others, *Constructing a Data-Driven Society*, p.415; Rogier Creemers, "Disrupting the Chinese State: New Actors and New Factors." Presented at the conference Digital Disruption in Asia: Methods and Issues, University of Leiden, 24-25 May 2016; and Katja Drinhausen and Vincent Brussee, "China's Social Credit System in 2021," p.19.

[84] He Huifeng, "China's social credit system shows its teeth, banning millions from taking flights, trains," *South China Morning Post,* 18 February, 2019, www.scmp.com/economy/china-economy/article/2186606/chinas-social-credit-system-shows-its-teeth-banning-millions.

[85] Chuncheng Liu, "Multiple social credit systems in China," *economic sociology_the european electronic newsletter,* 21-1, (November 2019) 22-32.

[86] Chuncheng Liu, "Multiple social credit systems in China," *economic sociology_the european electronic newsletter,* 21-1, (November 2019) 22-32. Also, Katja Drinhausen and Vincent Brussee, "China's Social Credit System in 2021," p.13.

[87] Katja Drinhausen and Vincent Brussee, "China's Social Credit System in 2021" p. 12.

[88] Stacie Hoffmann and others, *Standardising the Splinternet*, p. 250.

[89] Katja Drinhausen and Vincent Brussee, "China's Social Credit System in 2021" p. 12.

Contingency systems for the implementation of human rights can entrench discrimination and undermine a cardinal tenet of international human rights law: the principle of universality of human rights. This principle establishes that human rights are universal and everyone is entitled to their benefit without discrimination. In other words, the entitlement to human rights cannot be made contingent on the performance of responsibilities.[90] While China is not a party to ICCPR, it is a party to ICESCR and numerous other instruments that stress the universal nature of human rights. By making rights contingent on responsibilities, China would breach both civil and political rights, such as the right to freedom of movement (Article 13 UDHR, Article 12 ICCPR) and economic social and cultural rights such as the right to social security (Article 22 UDHR, Article 9 ICESCR[91]) as well as non-discrimination provisions (Article 2 UDHR, Article 2 ICCPR, Article 2 ICESCR).

In sum, the creation of a system which gives states the tools by which to make human rights and social benefits for each person contingent on their individual, closely-monitored behaviour has deeply worrying potential for human and societal control, would facilitate discrimination and runs directly contrary to the principle of universality of human rights.

4. Reinforcing Standards Development and Human Rights

Historically, standardisation was perceived as ethically neutral. However, as the example of New IP demonstrates, standardization processes can have important ethical and human rights implications.

Building human rights awareness into standardization is becoming ever more pressing, particularly as technology design challenges human rights and freedoms. If standardization processes approve technologies that undermine human rights, the norms and processes of human rights law do not offer a robust defence against implementation of those technologies. As in other fields, human rights norms fare poorly when competing against adopted technical standards. Trade protections afforded to ITU recommended standards provide a useful example. Under WTO rules, technologies standardized within ITU get immediate clearance to be traded internationally; the TBT agreement further encourages the adoption of approved standards. These WTO rules take precedence over human rights norms, even when standardized technologies may directly challenge human rights. Moreover, human rights norms and processes do not offer teeth by which to challenge technical standards. Not only is there no normative mechanism to embed human rights into standardization, but once adopted, standards cannot be set aside on human rights grounds. On the contrary, WTO rules support standardized technologies without consideration of their compliance with human rights.

If human rights continue to be overlooked in the development of technical standards, the standardization of surveillance-enabling technologies such as New IP has the potential to sweep away large swathes of the protections of the Universal Declaration of Human Rights and

[90] See UN Charter Art 55(c), UDHR Art 2, ICESCR Art 2, and ICCPR Art 2.
[91] See The Committee on Economic, Social and Cultural Rights (CESCR) General Comment 19 (2008) para 9.

the UN human rights treaties. Yet the government representatives, civil society, international organisations and academic community devoted to human rights may be oblivious, because they are not aware of or engaged in standardization processes.

It is vital that participation in SDOs diversify, and that it include participation from those concerned with human rights.

While standards development processes are expert-led processes and should remain a sphere of technical and engineering expertise, they should reinforce ongoing efforts to build a sufficiently open and diverse participation for there to be a realistic prospect of human rights issues being raised and considered in technology design. A recent ethnographic analysis of the IETF pointed to a cultural resistance among technical experts to include human rights considerations in standardization, rooted in shared views of technology as largely apolitical and "non- prescriptive" in nature.[92] In spite of the work of IETF's Human Rights Protocol Considerations Research Group, which has put forth human rights guidelines for protocol development, the organization has been slow to incorporate human rights considerations into standards.[93] Similarly, within ITU, proposals to introduce privacy assessments and human rights impacts reviews have received pushback.[94] Moving towards a greater integration of human rights into standardization processes will require the removal of participation barriers such as prohibitive costs, enhanced support to newcomers to reach the level of expertise needed to have a meaningful participation, and creative thinking to institutionalize human rights thinking in technical processes.

5. Recommendations

Like-minded governments should continue to increase their efforts to uphold the core values of a global, open and free Internet, and oppose ongoing efforts to standardise New IP and related technologies.

Given developments in technology and artificial intelligence, a growing range of technical standards processes engage ethical and human rights implications. Consequently, the authors make several specific recommendations with the aim of better integrating human rights into standards development.

- The human rights and diplomatic communities should, whenever possible, increase their participation in standardisation processes. Multilateral bodies such as ITU should lower barriers of participation for non-state members. Additional funding should be directed to

[92] Corinne Cath, "The technology we choose to create: Human rights advocacy in the Internet Engineering Task Force," *Telecommunications Policy*, Volume 45, Issue 6, 2021, (https://www.sciencedirect.com/science/article/pii/S0308596121000483).
[93] To date, only one protocol has been subject to a human rights review and solely for informational purposes. See IETF Memo entitled: "QUIC Human Rights Review," October 22, 2018. Beyond the cited guidelines, human rights considerations at IETF are mostly raised by individual participants through mailing lists and meetings.
[94] As reported by an anonymous source familiar with the ITU standardisation environment.

enhance the participation of human rights organizations and consumer protection agencies. At the same time, governments should consider bringing in human rights expertise into national delegations at multilateral bodies, including through non-governmental organizations.

- The UN should set up a unit on standards and human rights within OHCHR, tasked with advising technology SDOs on human rights issues and alerting the international human rights community to technology developments that require attention. OHCHR and standards bodies based in Geneva, such as ITU, should take advantage of their proximity to share knowledge and participate in each other's meetings.
- Human rights capacity and roles should be enhanced within the Secretariats and working groups of the SDOs. Existing groups, such as the IETF's Human Rights Protocol Considerations Research Group should be empowered to offer thorough scrutiny and advice on controversial technologies. Human rights analysis should be more thoroughly integrated into the workstream of technical working groups developing specifications and guidelines.
- Capacity building should be enhanced to bridge technical and human rights communities. Technical experts participating in SDOs should develop greater understanding of existing human rights standards and latest human rights guidance on surveillance technologies. Likewise, human rights and diplomatic communities should strengthen their awareness of technology development, Internet infrastructure and how SDOs operate. Events organized by SDOs could offer opportunities for both communities to interact through a combination of training sessions, workshops and panels.
- The UN Human Rights Council should commission a clear articulation of human rights standards regarding collation of data and surveillance, derived from Article 17 ICCPR and other relevant norms and building on OHCHR's existing work on privacy in the digital age, to more clearly delineate the distinction between technology that is and is not compatible with international human rights law.
- Consideration could be given to an international statement of commitment to human rights from Standards Development Organizations such that no standard is to be read as legitimating practices contrary to the human rights obligations of any State. Similarly, consideration could be given to revising the WTO rules so that their advantages do not apply to technology whose use would entail mass violation of human rights.
- Coordination efforts at the national level (e.g. through standards hubs) offer accessible entry-points for human rights groups to participate in standardization debates. When national standards hubs coordinate positions for standardisation discussions, they should encourage diverse participation, particularly in debates about technologies that have wide societal impact. Standards hubs should then feed those inputs into international standards development. Similarly, to encourage diverse participation, government delegates responsible for monitoring technology standards should act as an early warning system to alert civil society organizations when standards that have human rights impact are first proposed.