

Title	Chapter 1-II : Protecting individuals in the international battle of state v digital platforms : the importance of business and human rights approach
Sub Title	
Author	Thipsamritkul, Thitirat
Publisher	Keio University Global Research Institute
Publication year	2025
Jtitle	Monsterizing Platform Power and Law ; Volume 1. Platforms and States: How to Settle the Battle of Monsters ,p.27- 39
JaLC DOI	10.14991/KO11003002.00000001-0027
Abstract	
Notes	Chapter 1 : Actors of the governance of digital space
Genre	Book
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0027

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

PROTECTING INDIVIDUALS IN THE INTERNATIONAL BATTLE OF STATE V DIGITAL PLATFORMS

: The Importance of Business and Human Rights Approach

Thitirat Thipsamritkul*

1 Introduction

Professor Yamamoto proposed that states should recognise the independent and autonomous characteristics of platforms in the digital domain and establish a strategic relationship with them, i.e., an ‘agreement model’, under the control of constitutional mechanisms. This is similar to the current relationship between the US government and tech companies that possess superior technological power.

The agreement model does not advocate for the State’s total control over platforms in the ‘religion-politics congruence model’ as seen in the English church or current China. This model is more flexible than the ‘religion-politics separation model,’ in other words ‘digital secularism’, often reflected in the EU context since its main aim is not necessarily focusing on excluding the dominant power of non-state entities (the Catholic church in the Middle Ages and platforms today) from the political sphere and seeking to maintain the purity of its sovereignty.

This agreement model is crafted to balance the economic interest of cooperation with the protection of human rights or the rights of the people since it requires the protection of individuals by restraining the State’s power by constitutional mechanisms. Constitutional mechanisms are vital tools for safeguarding individual rights and upholding the principles of democracy. The concept of ‘digital sovereignty’, as advocated in this framework (and also in the ‘religion-politics separation model,’), is intrinsically linked to the protection of citizens’ rights by States.

However, ‘sovereignty’ may have a different meaning for other non-democratic countries. It is a fact in many countries that constitutional mechanisms do not always function to protect fundamental rights.¹ The

* **Thitirat THIPSAMRITKUL:** Lecturer of International Law in the Faculty of Law and Director of the Centre of Japanese Legal Studies at Thammasat University, thitirat@tu.ac.th

1 Helena Alviar García (eds), *Authoritarian Constitutionalism* (Edward Elgar, 2019).

interests of ‘individuals’ in non-democratic countries are not always the same as ‘national interests.’ This is in contrast with democratic States where ‘individual interest’ and ‘digital sovereignty’ are more closely intertwined.

Considering the extraterritorial effect of some economically developed States’ domestic regulations and the cross-jurisdiction impacts of the change of digital platforms’ internal rules, it is important to take an international approach that engages with the needs of ‘individuals’ and ‘civil societies’ in non-democratic contexts. Relying solely on domestic constitutional law may not suffice in protecting individual fundamental rights while overseeing the interactions between States and digital platforms.

Other international aspects may also be taken into consideration (such as geopolitical conditions, conflicts of law, and theory of jurisdiction), however, those will not be addressed here. This article will analyze the limitations of classic international law concepts when applied to the digital context. It will explore international human rights law as a potential framework to better understand and navigate the complexities of these State-platform relationships.

This perspective is particularly relevant in the international community, characterized by diverse types of Leviathan States. The discussion also highlights a fundamental conflict between the growing influence of international human rights law and the notions of sovereignty, which has been a cornerstone of the international legal order.

2 The Domestic approach is insufficient in analysing the State-platforms relationship

The claim of sovereignty by the State generally occurs in the international context. Its aims are mostly to preclude external threats, in other words, the intervention from other States. We therefore see States emphasize their sovereignty in territorial conflict, independent proclamation, and intervention in internal affairs. However, in the context of internal politics, the condemnation of foreign intervention is often a political discourse to alienate citizens who do not agree with governments.

These are the responses to ‘entities’ that threaten the supreme power of States to control their territory and people. We should try to understand what are such ‘threatening entities’ in the rising of digital sovereignty claims.²

(1) Variety of motivations behind the claim of digital sovereignty in 3 digital empires

For *Europe*, claiming digital sovereignty mostly means claiming State power to protect people’s freedom

2 Carol Soon and others, *Digital Sovereignty: State Action and Implications for Singapore* (Institute of Policy Studies 2023)

and privacy from commercial exploitation by foreign platforms which may also result in economic disadvantages. This is because those American platforms have a big influence on European citizens' lives but operate without much control by the American government. (This does not mean that Europe does not worry about Chinese platforms but they still do not seem to have as much weight in the discussion as Americans.³) In this sense, we may say that the protection of individuals matches with economic interests of European States.⁴ This is one of the reasons why the European approach is seen by some critics as a protectionist trade policy.

For *the US*, it may seem to be unnecessary to claim digital sovereignty since the American government can always exercise its power over the platform companies registered and operated in the US. Even with the recognition that any American measures on platforms will affect the whole world economically and socially, the platform issue can be discussed as a purely domestic legal problem. Internet freedom was framed to prevent regulation of platform business by the American government.⁵ The claim of digital sovereignty in the international sense occurred against the existence of Russian bot and Chinese applications suspected to be linked with governments, especially after a series of domestic digital legislations giving intrusive power to those governments came into force. The protection of digital sovereignty in the US means protecting democratic elections and people's free will.

Though both the EU and US are threatened by 'foreign platforms.' The EU is more worried about the American platforms that are under too few governmental regulations, while the US is more worried about the Russian and Chinese platforms that are under too much governmental control or may be used as the tools of governments.

The claims of digital sovereignty by Russia and China are also different. Their claims are rooted in the frustration that the internet has been full of American technologies. Moreover, the fundamental Internet governance rules and structures were created without the participation of any government, let alone the Russian and Chinese governments. It was the American tech communities and civil societies who actively dominated the field in the days internet was not yet the basic infrastructure of everyday lives either in the US or elsewhere. Therefore, it is no surprise internet ideology fits with the fundamental freedom protected in the spirit of Western liberal constitutions.

Russia and China wanted to take more roles in Internet governance since the 2000s. They were not very successful. They also tried to control how citizens in their domestic jurisdiction use Internet. China was successful in controlling technological infrastructure directly and became a techno-autocratic force.⁶ On the contrary, Russia could not do the same so it used State powers such as criminal penalties to indirectly limit how people use the internet. Russian and China's claims of digital sovereignty often appeared in opposition

3 Mathilde Velliet, 'Digital Sovereignty: European Policies, American Dilemmas' (*Notes de l'Ifri*, January 2023), <<https://www.ifri.org/en/publications/notes-de-lifri/digital-sovereignty-european-policies-american-dilemmas>>.

4 Rebekah Dowd, *Information Technology and Global Governance* (Palgrav Macmillan, 2022), 265.

5 Jack Goldsmith, 'The Failure of Internet Freedom: Probing the demise of a non-regulation, anti-censorship, global internet agenda' (*Knight First Amendment Institute*, 13 June 2018) <<https://knightcolumbia.org/content/failure-internet-freedom>>.

6 Anqi Wang, 'Cyber Sovereignty at Its Boldest: A Chinese Perspective' (2020) 16 Ohio St Tech L J 395.

to the liberal world order, which is made not only by the liberal States but also by international stakeholders who believe in free and open internet.

We can see that the 3 empires,⁷ the US, the EU, and China (and Russia) have claimed digital sovereignty for different motivations.

(2) Impacts on individuals in non-democratic countries

i Claiming sovereignty against its people

The claim of digital sovereignty is very alarming for people in the countries where ‘sovereignty’ has been used to control citizens, rather than to fight against external powers. Individuals in those countries are worried when;

- States have too much power to control platforms that enable more individual freedom,
- States have too little power to control platforms that exploit individual privacy and limit freedom,
- States conspired with platforms to control individuals.

Many governments who claim digital sovereignty are not seen to be truly worried about foreign platforms’ exploitation or foreign governments’ intervention via those platforms. Rather, their primary aim appears to be to restrict or manage their citizens’ engagement with these platforms to curb the rise in freedom, which often leads to increased expressions against the government. This trend is widely observed in multiple non-democratic countries.⁸

More anxiety comes with more legal transplants following the claims of digital sovereignty. The same model laws that these governments borrowed from European and North American countries may end up restricting people’s rights rather than enhancing them.⁹

For example, Thailand’s Computer-related Crime Act, which is modelled after the Cybercrime Convention, includes provisions that criminalize the introduction of malware and has been frequently interpreted as criminalizing the distribution of false information, leading to undue restrictions on freedom of expression.¹⁰ Thailand’s PDPA, which is modelled after the EU’s GDPR, is intended to balance privacy with the free flow of information, but it has often been used as an excuse by state agencies to prevent the disclosure of information or to block individual access to information. This misinterpretation of PDPA is seen by many practitioners as an obstacle to open government agenda and the protection of

7 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP, 2023).

8 Anupam Chander and Haochen Sun, ‘Sovereignty 2.0’ (2022), 55 Vand J Trans L 283.

9 Chander, Anupam, “When the Digital Services Act Goes Global” (2023). Georgetown Law Faculty Publications and Other Works 2548. <<https://scholarship.law.georgetown.edu/facpub/2548>>

10 For general evaluation of Thai Computer Crime Act to the standard of the Cybercrime Convention: Sinfah Tunsarawuth and Toby Mendel, ‘Analysis of Computer Crime Act of Thailand’ (2010) *Center for Law and Democracy*, <http://www.lawdemocracy.org/wp-content/uploads/2010/07/10.05_Thai_.Computer-Act-Analysis.pdf>. For more detailed comparison between art.7 of Cybercrime Convention (Computer-related Forgery) and the section 14 of Thai Computer Crime Act: Santipatn Prommajul, “The criminal justice response to cybercrime: Thailand.” (2008) <https://unafei.or.jp/publications/pdf/RS_No79/No79_13PA_Prommajul.pdf>.

accused persons.¹¹ Moreover, there is concern that the 2022 Royal Decree on Digital Platform Services, which seeks to follow the direction of the EU's Digital Service Act, might provide more convenient tools for governmental agencies to arbitrarily intervene with foreign digital platform providers through the process of mandatory registration and content takedown order. This may eventually bar Thai citizens from accessing DPF.¹²

ii Limited capacity of non-technologically advanced States

In addition, even if States have genuine goodwill to protect their individuals from exploitation by platforms, \ States' power still affects the level of individual protection. While states theoretically possess the sovereign authority to regulate foreign digital platforms through domestic law, the actual effectiveness of this power varies based on each State's economic influence and geopolitical realities. Internet business does not need strict approval from states in the same manner as oil or gas companies, except for China. The true regulatory authority is mostly confined to jurisdictions where digital platforms are headquartered (such as the US) or hold significant market presence with normative powers (such as in the EU¹³).

Considering this difference in States' power in relationships with platforms, the domestic constitutional mechanism constraining such relationships alone cannot sufficiently protect citizens' rights. The authoritarian States may be unwilling and unable to control the platforms. We shall look for the tools available in international legal order that may restrain the power of both States and platforms that may affect individual rights.

3 International approach

(1) Failure of classic multilateral cooperation

The classic multilateral system of international law never successfully put control of internet governance in the hands of States, except for the physical infrastructure-related issues, such as the International Telecommunication Union (ITU)'s regulation, which does not confer States much power to regulate how people use internet. Compared to other emerging areas like outer space and environmental law, cyberspace has remained largely unregulated by states and international bodies.

Internet governance has been led by the 'Internet Corporation for Assigned Names and Numbers' (ICANN), a collective of engineers, lawyers, human rights activists, and some state representatives. ICANN's approach leans towards liberal values has prioritised individual freedom and prevented unjust attempts of intervention by States, at least to a certain extent. Nevertheless, the scope of ICANN's governance is limited

11 Sitthikarn Theerawatanachai, 'Laak Tassana Ruang Kormoon Satarana (Open Data) Pretetthai'(Elect, Mar 2021) <<https://elect.in.th/open-data/>>

12 Article 19, 'Thailand: Content takedown rules will undermine free expression online'(December, 2022) <<https://www.article19.org/resources/thailand-content-takedown-regulation/>>

13 Anu Bradford, *Brussel Effects: How the European Union Rules the World* (OUP, 2020).

to the protocol layer, not the content layer.¹⁴

The United Nations has tried to play a role in cyber peace and security, leading to the ‘World Summit on the Information Society’ (WSIS) in the 2000s. However, it has not significantly given States control over the internet, with the UN’s actions leaning towards the call for cooperation rather than agreeing on any substantive law through the process of negotiating different interests.¹⁵ This is clear when we look at what States have agreed at the ITU were the undisputed rules governing basic hard infrastructure. All states want the same stable connections with no unnecessary interference. States never agree on how to regulate the top layer of the internet such as protocols or contents layers.¹⁶

It is understandable because the UN is based on the common fear of WWII. WTO is based on the common desire to trade and it could only engage China after China has shifted to embrace some capitalist ideas. A miracle of the Universal Declaration of Human Rights happened only after the cruel scale of the killing, the Nazi holocaust. Human Rights Courts only exist in regions that share similar cultural and political characteristics, not in Asia. Furthermore, comparing the UN to the EU, we can see that the relative similarity among European nations is the secret sauce in producing common norms at the supra-national level.

Since states are too different, we can expect very little from the multilateral frameworks of cooperation. The existing UN frameworks are based on some common interests between states. While the efforts in traditional intergovernmental cooperations fell short of granting States the power to control internet, the protection of individuals’ online freedom has become an important concern of international human rights bodies.¹⁷

Today, the UN’s ‘Global Digital Compact’ (GDC) policy¹⁸ aims to create a framework for using technology for sustainable human development, focusing on three main areas: i) closing the digital divide, ii) connecting various internet stakeholders to harmonized approaches, as tech companies largely self-regulate, and iii) aligning common norms with the principles of freedom and human rights.

(2) Limitation of classic international human rights law

International human rights law has been trying to prevent violation of human rights by both state and non-state actors. Its mechanism works through international diplomacy, i.e. State mechanism. International human rights law originated in treaty-making, the legal tool that States use to protect their national interest. However, unlike other types of treaties, international human rights treaties have a distinct aim to protect individual interests, which may not be the same as the national interests of several States.¹⁹

The concept of international human rights law itself is a direct challenge to the classical concepts of Inter-

14 Jovan Kurbalija, *Introduction to Internet Governance* (DiploFoundation, 2016).

15 Liisi Adamson, ‘International Law and International Cyber Norms A Continuum?’ in Dennis Broeders Bibi van den Berg (eds), *Governing Cyberspace Behavior, Power, and Diplomacy* (Rowman & Littlefield, 2020).

16 William Dutton and Malcolm Peltu, ‘The emerging Internet governance mosaic: connecting the pieces’ (2005), Forum Discussion Paper No.5, Oxford Internet Institute.

17 Molly K Land, ‘Toward an International Law of the Internet’ (2013) 54 *Harvard International Law Journal*.

18 UN, *Global Digital Compact Policy Brief* (2023) <https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Policy_Brief_Infographics_2.pdf>.

19 Matthew Craven, ‘Legal Differentiation and the Concept of the Human Rights Treaty in International Law’ (2000) 11 *EJIL* 289.

national law; which are “territorial state sovereignty” and “non-intervention” principles. It has transformed the domestic relationship between the State and its citizens to become an international issue. This is justified by such State’s consent to be bound by the universal norm written in the treaty.

This ambition to protect individual rights went beyond the classical framework of State consent when we look at the method of evolutionary interpretation that allows human rights treaties to be “living instruments” that expand the protection of rights in the digital era.²⁰ Nevertheless, human rights treaties are still located in the UN system which is not equipped with strong tools for enforcement. This is the inherent nature of a multilateral system depending on the voluntariness of equal sovereign States to create and also enforce international norms. States are free to choose their actual level of compliance despite their words of commitment in the international sphere. Therefore, human rights scholars and practitioners always emphasized the importance of internalising human rights norms into domestic legal systems. The sustainable change for human rights protection must come from local societies. External pressure from the international community can only help in supporting the initiatives and acceleration.

(3) Opportunities in the Business and Human Rights Framework (soft law)

Facing the limitation of protecting human rights through States’ measures, the international human rights community shifted to promote human rights protection through multinational business actors whose conducts affect individual rights across borders. Following the global movement of corporate social responsibility in the 1990s,²¹ the UN Guide on Business and Human Rights (UNGPR) opened a new channel for human rights advocacy.

The human rights impact of multinational enterprises has more direct effects on individuals in various areas, ranging from labour rights to environmental interests. The directness of human rights impact increased when it comes to consumers’ data privacy and online freedom of expression because tech companies have technological tools to effectively interfere with the behaviour of individuals who “live” on their platforms. This algorithmic interference by these digital landlords can be much more effective than the governmental power to police and regulate citizens’ behaviour in their territories.²²

Before UNGPR, the international community prevented businesses’ violation of human rights through the mechanisms of State law. It had to rely on the host and home States’ willingness to regulate transnational businesses which can be easily influenced by changes in national economic interest. Some States may be reluctant to enforce labour regulation because it will lose the comparative advantage of “ease of doing business” and push the foreign direct investment away from the country.

The UN mechanism to enhance human rights protection by business did not become stronger after UNGPR, but multinational businesses in general have more incentives than States to accept human rights

20 Molly K Land, ‘Toward an International Law of the Internet’ (2013) 54 Harvard International Law Journal.

21 Mauricio Andrés Latapí Agudelo and others, ‘A literature Review of the History and Evolution of Corporate Social Responsibility’ (2019), 4 International Journal on Corporate Social Responsibility 1.

22 Lawrence Lessig, *Code 2.0* (Basic Books, 2006); Jack M. Balkin, ‘Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation’ (2018), 51 UC Davis Law Review 1149.

principles. Different from States, corporations cannot invoke the argument of “internal affairs” or “sovereign freedom” to deny international criticism of their conduct. The only possible argument that corporates may raise would be that States are the main duty bearers of human rights protection and corporates’ main aim is private profit maximization, not collective social welfare. However, it is not easy for corporates to proclaim such an argument out loud. Such a claim sounds illegitimate in the eyes of their consumers and other stakeholders. Corporates today need to act or at least pretend to act that they care more than just simple profit maximisation.

The soft law framework of “business and human rights” including naming and shaming, is therefore very powerful for corporates to guide their conduct and for civil societies to criticize undesirable corporate behaviours. Furthermore, when applying this idea to digital platforms companies that have more direct and broader impacts on people’s lives, the effectiveness of this international soft law may exceed domestic legislation. The tech companies, including those in China, do not dare to take a stance opposing their users’ interests. It is not exaggerated to say that the “consumer-company tie” might be even stronger than “citizen-State tie” in some non-democratic countries. In many cases, the interests of individuals align with the interests of tech companies than those of authoritarian States.

We should not disregard the relationship between individual users and digital platforms just because they are not bound by democratic means. Indeed, users are not citizens of digital platforms, but the legitimacy (or at least effectiveness) of protection does not come solely from the democratic origin. In the case of digital platforms, we should consider the fact that users are their invaluable assets, both as the source of input data and as the base for attention merchants to claim revenue from ads. Their engagement and participation underpin the operational and economic success of these platforms.

4 Non State-centric approach

(1) Examples of digital platforms as protectors of individual rights against their national sovereigns

There are cases where tech companies acted as “keepers of international law”²³ against the will of States to ignore the same international obligations. Some companies provided technological tools that helped individuals to fight against authoritarian States.

i Against State’s manipulation of platforms: NSO litigation and information operations investigation

WhatsApp and Apple filed similar lawsuits against the NSO Group, an Israeli spyware maker company, for the exploitation and misuse of their platforms to deliver Pegasus spyware to various activists’ and journalists’ phones. These services by NSO Group were done for various governments that wanted to surveil and

23 Jay Butler, ‘The Corporate Keeper of International Law’ (2020) 114 ASIL 189.

oppress individuals and civil societies.

WhatsApp initiated this lawsuit to protect user privacy and the integrity of its platform.²⁴ Corporate social responsibility links directly to the platforms's commercial interest in this case. Apple also declared a broader aim to combat State-sponsored misuse of surveillance technology and human rights abuses, by committing to contribute its damage from this case to support research and advocacy groups working on cyber surveillance issues.²⁵

The companies in these cases are playing the role of “protecting” not only their users but also the digital welfare of the general public in other countries.

A similar protection of general online freedom of expression can be seen in Meta and Twitter's investigation of information operations by States. States around the world use and manipulate platforms to distribute information and misinformation. The revelation of platform manipulation (in Twitter's terms) and Coordinated Inauthentic Behavior (in Facebook's terms) by states led to account takedown and many litigations in various jurisdictions including Thailand, Iran, Hongkong, Philippines, etc.²⁶

ii Multistakeholder-initiated industrial standard: GNI

Global Network Initiative (GNI) is a multistakeholder platform comprising information and communications technology (ICT) companies, human rights and press freedom organizations, academics, and investors. It aims to enhance the protection of freedom of expression and privacy on technology platforms to be aligned with international human rights standards. Its implementation guidelines include many measures to prevent governmental arbitrary interference.²⁷

Many tech companies' transparency policies follow this standard. For example, in 2023 Meta announced a new transparency policy to show that contents were taken down by the governmental request.²⁸ It also planned to share copies of governmental requests with the public.²⁹ Its main reasons are “informing public discourse, facilitating research and journalism, and enabling people to hold their governments accountable.” The criteria of UN Guiding Principles on Business and Human Rights is to be followed when it has to prioritise issues. It also published the first human rights report for the 2022 year performance.

Facebook and many DPFs revealed the statistics of governmental requests quietly for many years but very few customers knew about it or were aware of such fact that DPFs resisted arbitrary governmental power. This kind of transparency measure taken by digital platforms will nudge individual users to notice the State-platforms relation. It will open the way for citizens to check and hold both State and platforms accountable under human rights principles, either by filing complaints to the domestic constitutional rights

24 Jonathon Penney and Bruce Schneier, 'Platforms, Encryption, and the CFAA: The Case of WhatsApp v NSO Group' (2021) 36 Berkeley Technology Law Journal 101.

25 'Apple sues NSO Group to curb the abuse of state-sponsored spyware' (Apple Press Release, 23 November 2021) <<https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/>>.

26 Camille François and evelyn douek, 'The Accidental Origins, Underappreciated Limits, and Enduring Promises of Platform Transparency Reporting about Information Operations' (2021) 1 Journal of Online Trust and Safety.

27 GNI Implementation Guidelines <<https://globalnetworkinitiative.org/implementation-guidelines/>>.

28 Statistics of each country <<https://transparency.fb.com/reports/government-data-requests/>>

29 Meta, 'How we assess reports of content violating local law' <<https://transparency.fb.com/data/content-restrictions/content-violating-local-law>>

protection mechanism, or under international mechanisms such as Universal Periodic Review (UPR) and individual communication system under UN human rights treaties.

One example of the public communication of Meta about arbitrary government requests could be seen during the highest moment of the youth movement in Thailand. In 2020, the Thai government ordered Facebook Thailand to close a group of 1M members called “Royalist Marketplace”, a group where political reform was discussed actively with the background of the 2020 youth movement. Facebook decried that the government threatened to sue its Bangkok office so it needed to close the group but announced that it would legally challenge such an order. Such litigation never happened but Facebook allowed a new group to be formed.³⁰ The new group could attract even more people to join in a few days. In this case, the governmental order was not directly obstructed by the platform but the illegitimacy of such action was announced publicly by the platform to international media and the human rights community.

iii Direct responsibility of private companies: Amnesty report on Rohingya

Following the UN and other international organisations’ effort to conduct factfinding about the role of the social media platform in the 2017 Rohingya tragedy,³¹ Amnesty International published a report calling for Meta to give remedies to the Rohingya community based on UNGP regarding the individuals’ rights to remedy and corporates’ responsibility.³²

Though Meta rejected to give a direct remedy and is facing litigations,³³ after 2017, it has improved Myanmar language competency, technology to detect hate speech and internal policies to prevent harm that may be derived from its social media platform.³⁴

This implies the understanding that to comply with international law, tech companies must not allow their platforms to be used by States to violate the rights of their citizens.

(2) Limitation of non-state centric approach under international human rights framework

The abovementioned examples illustrate that digital platforms have an awareness of their capacity to protect the fundamental rights of their users. They refuse to comply with illegitimate requests of governments that may interfere with the privacy and freedom of users, or at least expose such requests in the case they cannot refuse. They do not only comply with the company’s ‘duty to respect’ their user’s rights as recommended in UNGP, but they also ‘protect’ their users and the general public by taking further steps to prevent or minimize the government’s abusive use of their platforms that may result in negative human

30 Patpicha Tanakasempipat, ‘After block, new Facebook group criticising Thai king gains 500,000 members’ (Reuters, 25 August 2020) <<https://www.reuters.com/article/thailand-facebook-idUKL4N2FR2PB>>.

31 UN Human Rights Council, Independent International Fact-Finding Mission on Myanmar <<https://www.ohchr.org/en/hr-bodies/hrc/myanmar-ffm/index>>.

32 Amnesty International, *Myanmar: The social atrocity: Meta and the right to remedy for the Rohingya* (2022) <<https://www.amnesty.org/en/documents/asa16/5933/2022/en/>>.

33 Catherrine Sanz, ‘Rohingya refugees move to have claims against Meta heard in Irish court’ (Business Post, 25 August 2023) <<https://www.businesspost.ie/news/rohingya-refugees-move-to-have-claims-against-meta-heard-in-irish-court/>>.

34 Rebecca Hamilton, ‘Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators to Commit Atrocities’ (2022), 63 Boston College Law Review 1349, 1403.

rights impacts for society at large.³⁵ This ‘duty to protect’ is originally seen as a governmental function, the important first pillar of UNGP.³⁶ Some States do oblige companies to do these protective functions via their national laws. The extraterritorial effect may result in protecting citizens of other States.

The reliance on voluntary commitments for protecting ‘fundamental rights’ draws considerable skepticism and criticism, particularly because it hinges on the ‘willingness’ of companies. At times, the effectiveness of these commitments boils down to the readiness or capacity of specific employees to uphold them. Given the high turnover rates among tech company staff, this approach hardly seems like a steadfast method for ensuring human rights. However, we should not forget that the implementation of international human rights treaties also depends on the State’s willingness and officials’ capabilities.

The GNI standard played a significant role in reducing this discretion and setting the expectation for what platforms should do to ‘respect’ their users. It announces collectively that private companies, even subject to the domestic jurisdiction of States, will not just blindly follow the request of States without questioning its legitimacy under international human rights standards. Even in the case that tech companies, especially those who have less bargaining power, may choose to follow the interpretation of States on what constitutes legitimate requests or interventions, they still need to expose such requests and interventions to the public. The practice of transparency reports become a powerful tool for civil societies to hold governments accountable, at least in countries where parliamentary and/or judicial organs still function to check the executive branch.

On the contrary, the level of active steps that each company may take to ‘protect’ such as in the case of NSO litigation and information operations research, fully depends on resources, human capacity and willingness of the company.

It is clear from the case of Amnesty International’s report that requesting ‘remedy’ from platforms by solely relying on international legal grounds is still practically hard to pursue. If international NGOs want to push for actual compensation, they must rely on States’ judicial power to order so.

The non-democratic nature of platform companies is another great point of criticism. The acquisition of Twitter by Elon Musk showed how fragile platform policy may be. Twitter, now X, has seen significant changes in content moderation, with about 30% of its Trust and Safety staff, key to these efforts, being laid off.³⁷ This approach, reflecting Musk’s “free speech absolutist” stance, may not fully align with international standards. This reduced moderation, including disinformation monitoring during election periods, could lead to a surge in harmful content and negative impacts on users. Many activists no longer consider X as a safe, democratic space for public discourse.

35 “UNGP Commentary to Principle 13.<https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciples-businesshr_en.pdf>”

36 See ‘Mandatory Due Diligence’ at Business and Human Rights Resource Centre Website <<https://www.business-humanrights.org/en/big-issues/mandatory-due-diligence/>>

37 Sheila Dang, ‘X reorganizes trust and safety team under Musk, CEO Yaccarino’ (Reuters, 1 August 2023) <<https://www.reuters.com/technology/x-reveals-reporting-structure-under-elon-musk-ceo-yaccarino-2023-07-31/>>; Vittoria Elliot and David Gilbert, ‘Elon Musk’s Main Tool for Fighting Disinformation on X Is Making the Problem Worse, Insiders Claim’ (Wired, 14 October 2023) <<https://www.wired.com/story/x-community-notes-disinformation/>>.

The OpenAI board members saga also alarmed us that corporate governance may affect the direction of technological development of an important innovation such as generative AI tool widely used across the globe. The weight of ethical and human rights standards of AI research and application may be changed by the decision of a handful group of people.³⁸

5 Conclusion

(1) Individual freedom at the center

I have argued that the relationship between users and DPFs necessitates a nuanced understanding of digital sovereignty. If the goal of contemplating the relationship between States and platform is truly about protecting the rights of individuals, we increasingly need to move beyond state-centric thinking because we cannot escape the reality that states are diverse and do not equally protect the freedoms of individuals.

The fundamental rights of individuals outside the developed world should be taken into account in the current debate on the State-platforms relationship. The model of relationship that assumes constitutional mechanisms cannot be simply applied in non-democratic countries. An international approach has to be taken.

Therefore, instead of asking how states can regulate platforms to most benefit the protection of citizens' freedoms, we might pose a new question: "What tools do citizens have to protect their own freedoms? A domestic constitutional mechanism that guarantees freedoms is just one of the options citizens have to protect themselves from threats or infringements by platforms. On the other hand, platforms' codes of conduct based on international human rights law offer another option for citizens or users to protect themselves from threats or infringements by States.

(2) International responsibility of platforms

As discussed earlier, international human rights 'hard law' based on State consent has inherent limitations as seen in the different levels of implementation in each State. The non-State-centric approach of international human rights law, such as UNGP, may provide some solutions by directly setting collective standards for platforms to 'respect' their user's rights and encourage them to take steps in utilising their technological resources to 'protect' the human rights of individuals in society at large. Nevertheless, the remedy from platforms for individual victims still needs domestic judicial functions to help.

Therefore, It is important to pressure digital platforms to recognize their international human rights obligations, "independently of States' abilities and/or willingness to fulfil their own human rights obligations."³⁹

38 Charles Duhigg, 'The Inside Story of Microsoft's Partnership with OpenAI' (The New Yorker, 1 December 2023) <<https://www.newyorker.com/magazine/2023/12/11/the-inside-story-of-microsofts-partnership-with-openai>>; Amba Kakarchive and others, 'Make no mistake—AI is owned by Big Tech' (MIT Technology Review, 5 December 2023) <<https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/>>.

39 UNGP Commentary to Principle 11. <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf>

A proposal for an international treaty on platform regulations cannot provide more realistic human rights protection either because treaty-making fora is often a place for States' interest negotiation. The majority of States who called for a multilateral digital treaty so far dismissed the multistakeholder approach and raised digital sovereignty to strengthen their domestic power to control people, not to enhance freedom.⁴⁰

The only multilateral framework that aims to protect individuals is the international human rights treaties that bind States and businesses under the same principles to care about their citizens and consumers, though at different levels of obligations. Stakeholders in internet governance are already familiar with international human rights standards. It sounds more legitimate for ICANN to rely on universal standards like UDHR rather than any country's law. Facebook's Oversight Board, a separate entity that reviews the company's decisions relating to freedom of expression, also rely on international instruments like ICCPR, not the American constitution. International human rights norms become common a benchmark for industry players applying to all users across the globe equally, contrasting with the fact that the same norms are interpreted and implemented very differently in each State.

In conclusion, platforms do not only provide space for users to resist the State's arbitrary power but also need to protect users from the State's coercive interference in exercising their rights. As long as we cannot expect a similar satisfactory level of constitutional constraints on digital platform regulations in each State, the discussion of the State-platforms relationship must not omit the legal form and structure of the platform's responsibility to respect international human rights standards.⁴¹

40 Tom Ginsburg, *Democracies and International Law* (CUP, 2021) 225-229.

41 Agnes Callamard, 'The Human Rights Obligations of Non-State Actors' in David Kaye (Eds), *Human Rights in the Age of Platform* (MIT Press, 2019); Neli Frost, 'Out with the 'Old', in with the 'New': Challenging Dominant Regulatory Approaches in the Field of Human Rights' (2021) 32 EJIL 507; Edoardo Celeste and others, *The Content Governance Dilemma: Digital Constitutionalism, Social Media and the Search for a Global Standard* (Palgrav Macmillan, 2023).