Stanford | Global Digital Policy Incubator
*Cyber Policy Center*

# GLOBAL DIGITAL POLICY SNAPSHOT

## HUMAN RIGHTS AND GOVERNMENT REGULATION OF DIGITAL PLATFORMS

SEPTEMBER 2020

**INSIDE THIS BRIEF:**



## INTRODUCTION

Digital platforms play an increasingly central role in both the exercise of human rights and the evolution of new threats to these rights globally.The growing influence of such platforms compounds the urgency to address problems such as the proliferation of disinformation, their use by extremist organizations, and opportunities for malign actors to manipulate algorithmic recommendation systems and other features of digital technologies for their own purposes. Policymakers have an obligation to check the growing powers of commercial platforms and to tackle the potential harms they pose to society. Yet, many of the initial attempts in this space have failed to fully balance a need for regulation with the need to protect human rights. In seeking an approach that will respect human rights when solving the pressing problems posed by digital platforms, it is critical that governments not restrict free expression, invade users' privacy, or undermine the right to appropriate redress for harms. This brief snapshot considers the current state of global regulation, and suggests steps forward for a rights-respecting approach to the governance of digital platforms.

# LANDSCAPE OF GOVERNMENT REGULATION OF DIGITAL PLATFORMS

There is substantial variation in how governments around the world have approached regulating digital information platforms, but the obligations placed on platforms fall largely into three main categories: obligations to remove content, obligations to retain/share user data, and obligations for data localization.

**Obligations to Remove Content**

Often framed as targeting hate speech, fake news, or other problematic online speech, one approach that governments have taken to regulating platforms is by imposing obligations on platforms to remove content, often on a short time frame. The first and perhaps most influential example of this kind of regulation is the German Network Enforcement Act, commonly known as NetzDG. The law, passed in 2017, requires that platforms with at least 2 million users establish processes for users to report illegal content, and requires that any "obviously illegal" content be removed within 24 hours of receiving a complaint, and other illegal content within 7 days. Although the law applies only to content which is illegal in Germany, there has been substantial concern that requiring removal on such short time frames would lead platforms to remove legitimate speech in an attempt to avoid penalties. Additionally, it places the burden of determining the legality of content onto platforms, rather than on the governmental or judicial bodies that should typically make such determinations.

While the German law was focused on content already illegal under German law, other countries have since passed laws that target content that might otherwise not be illegal. For example, in Singapore, platforms can be obligated to remove or label content that the government determines to be "false statements of fact" that threaten Singapore's national security, "public tranquility" or relations with other countries. This content might not be fundamentally illegal under Singapore law, but is required to be removed or labeled by platforms at government request. The types of content are also quite broad and not clearly defined. This is another common trend in these types of laws, and can lead to opportunities for governments to repress legitimate speech.

Since the passage of NetzDG, a number of other countries have passed regulations based on or inspired by the law. This has included a recent French law, the majority of which was struck down by the French Constitutional Council, as discussed below. It has also, however, included a number of laws in authoritarian countries, including in Russia and Venezuela which have used the model of NetzDG to justify repressive laws in their own countries. These laws pose potential risks to human rights even in established democracies, but the diffusion of such policies to countries without democratic checks on government power are even more troubling.

**Obligations Around User Data or Identification**

Laws that place obligations on platforms around user data or identification are often framed in terms of national security or the need to properly investigate crimes. These laws sometimes require platforms to retain user information, messages or other data, either indefinitely or for a set period of time. In some cases, like in China, laws can require that users' real names be linked to their online behavior to ensure the ability for the government to track content back to specific individuals.

A Brazilian law which is currently being considered, would require private messaging platforms to retain any messages shared by more than 5 people reaching at least 1000 people for 3 months. Earlier drafts of the bill contained even more substantial requirements to retain data, and human rights advocates have asserted that even this more limited requirement will in practice mean that platforms have to retain data on most posts, because they cannot predict which will be viral enough to meet the standard.

**Obligations for Data Localization**

A final major trend in the regulation of digital platforms is the introduction of requirements for data localization. These laws require that platforms store user data for a given country within that country. This could seem like a technical requirement, but such regulations give governments substantial increased control over the data of their citizens. It also forces the data to be covered by the local jurisdiction, which particularly in the case of authoritarian regimes. For example, a recent Turkish law that requires platforms to store data of Turkish citizens in Turkey, jeopardizes data privacy and casts doubts on whether individual user data will be protected from government intervention. The law comes as part of a broader set of policies aimed at tightening government control over the internet, and the data localization requirement has raised serious concerns over increased government interference with online expression.

# HUMAN RIGHTS RISKS & IMPLICATIONS

While it is important for governments to ensure that internet companies do not operate beyond the reach of the law, regulating information and communications platforms implicates a number of significant human rights considerations for which policymakers must account. These rights include (but are not limited to) freedom of expression; access to information; the right to due process; freedom of assembly; and the right to privacy.

**Freedom of Expression**

Digital platforms globally have become important instruments for sharing ideas, opinions, and other information. Such forms of speech and expression are often the primary purposes for which digital platforms are used. Freedom of expression––as enshrined by Article 19 of the Universal Declaration of Human Rights––is foundational to the human rights framework, and may be directly implicated (and potentially undermined) by certain approaches to regulating digital platforms. Such risks to freedom of expression are particularly acute in the context of regulations concerning the removal of online content. France's recent law regulating online hate speech, for example––which required large platforms to investigate and remove certain categories of illicit content within either 24 hours or face substantial fines––was largely struck down by the French Constitutional Council in recognition of the risks the law presented to free speech. Among other concerns, the Council agreed with rights advocates that the law's requirement of companies to assess and remove content on short timelines under the threat of severe sanctions risked incentivizing platforms to be over-cautious by removing or blocking even legitimate speech in order to avoid penalties. In other cases, such as in Singapore, the laws do not clearly or narrowly define the content categories which must be removed. Ambiguity risks incentivizing platforms to remove any content that the government might find objectionable, and also positions governments to abuse their interpretation of these vague definitions for censorship purposes.Particularly as many governments seek to implement laws addressing digital disinformation, policies must be balanced against the importance of free expression. Underscoring this point, a collection of digital rights experts recently issued an expansive report under the aegis of the ITU & UNESCO Broadband Commission for Sustainable Development, which concludes that "disinformation cannot be addressed in the absence of freedom of expression concerns," and that "actions to combat disinformation should support, and not violate, this right."

**Right to Due Process**

Certain platform liability laws require content to be removed in the absence of any judicial determination as to the content's legality, and without sufficient guidance or standards to inform the implementation of these removal practices among private companies. The guarantees of procedural fairness and due process of law are important elements of the right to equality before courts and tribunals, which is afforded under Article 14 of the International Covenant on Civil and Political Rights (ICCPR). By outsourcing to private companies the responsibility for making legal determinations about speech and other content, these laws undermine the due process rights of users whose speech may be censored.This risk has been cited frequently, for example, by critics of Germany's NetzDG law, whose provisions require large digital platforms to evaluate and take action against certain categories of illegal content (in some cases within 24 hours) without any judicial determination as to the content's legality, and with no recourse for users whose lawful content is removed pursuant to the regulation. In other cases––including China, Russia, and France––platform liability laws have empowered state authorities to request offending content removal without court orders or other independent adjudicatory hearings where affected parties could seek redress. International standards require that liability should only be imposed where a platform or other digital intermediary has refused to comply with an order from an independent, impartial, authoritative oversight body, such as a court.

# HUMAN RIGHTS RISKS & IMPLICATIONS, CONT.

**Freedom of Assembly**

The freedom of peaceful assembly is a well established human right––reflected in the Universal Declaration of Human Rights and the ICCPR, as well as in other international standards––which is now commonly exercised across, or facilitated through the use of, digital platforms of all kinds. Regulation of digital platforms carries the potential to undermine freedom of assembly both online and offline, as governments have used internet restrictions to impede protests, and to scrutinize associations and other online connections––a trend that the International Center for Not-for-Profit Law documented as early as 2011. These risks are illustrated, for example, by China's application of its cybersecurity and national security laws across digital platforms in Hong Kong. Observers have noted that Beijing has been sensitive about the potential for internet applications being used for discussions that could lead to organized action on the streets. New rules implementing China's national security law in Hong Kong, have included regulations that give the police powers to take down internet posts and punish internet companies that do not comply with requests for user data (applied globally), which may potentially be used as evidence to imprison users for participation in pro-democracy activities. The rules explicitly give the authorities the ability to jail employees at internet companies if the firms do not comply with such data requests, and many large digital platforms have announced that they are halting the processing of data requests out of concern for the risk to activists' human rights.

**Right to Privacy**

Government regulations impacting digital platforms can carry risks to users' privacy, an important element of the international human rights framework. The right to privacy often carries implications for the exercise of several human rights––including freedom of expression (advocates at Privacy International have framed privacy and expression as "two sides of the same coin") and freedom of movement, particularly where access to one's personal data or communications can be used to surveil one's physical whereabouts. In the digital realm, the relationship between and among these rights warrants important consideration among policymakers imposing liabilities upon digital platforms. The recently proposed legislation targeting disinformation in Brazil, for example, would impose new responsibilities and liabilities upon certain platforms that could have important consequences for user privacy. The proposed law would compel private messaging applications to retain, for three months, the chain of all communications that have been "massively forwarded." This requires companies to store large amounts of metadata of users' personal information and communications, or break encryption to get access to an encrypted message, which rights advocates argue will violate users' expectation of privacy. The IACHR Special Rapporteur for Freedom of Expression advises that privacy should be understood "in a broad sense as every personal and anonymous space that is free from intimidation or retaliation, and necessary for an individual to be able to freely form an opinion and express his or her ideas as well as to seek and receive information, without being forced to identify him or herself or reveal his or her beliefs and convictions or the sources he or she consults." Laws that require digital platforms to retain or reveal users' personal information or communications risk undermining important freedoms.

**Access to Information**

Like privacy, the freedom to access information often relates to the exercise of other human rights, perhaps most notably the freedom of expression. Indeed, the IACHR's Declaration of Principles on Freedom of Expression states that, "[a]ll people should be afforded equal opportunities to receive, seek and impart information by any means of communication without any discrimination…" In the digital context, the Special Rapporteur on Freedom of Expression indicates that this principle requires removing arbitrary barriers to––and promoting the greatest possible access to––digital technologies and infrastructure, as well as "to the greatest possible amount of information available on the internet."Governments seeking to develop platform liability laws should be cautious to avoid outcomes that may result in curtailing citizens' access to information online. For example, Pakistan unveiled a set of internet rules earlier this year that featured severe penalties for digital platforms that failed to comply, including potentially shutting down their services. The threat of this outcome, in turn, led several tech companies to threaten to preemptively cease operations in the country, depriving Pakistanis of key online resources. Such outcomes not only diminish local citizens' access rights, but risk contributing to the greater fragmentation of internet access globally.

# RECOMMENDATIONS FOR POLICY MAKERS

***Governments should:***

- **Not rely on platforms to make determinations about the legality of content, or in other ways outsource judicial or governmental authority to private companies.** The regulation of digital platforms should subject questions of legality to the determinations of an independent, impartial, authoritative oversight body. Failure to do so risks enabling the privatization of censorship.

- **Provide clear, narrow definitions for any content categories or specific problems to be addressed by platform regulations.** Specificity is necessary to mitigate the risk of over-broad interpretations that may result in unintended censorship or implementation that is either overly restrictive of user rights or overly extractive of user data.

- **Ensure opportunities for civil society engagement and consultation with human rights experts when crafting regulation of digital platforms.** Policy development processes should include multi-stakeholder engagement prior to the formulation and implementation of laws regulating digital platforms, and include an impact assessment regarding consequences of the regulation on freedom of expression, freedom of assembly, due process rights, and rights to privacy and access to information.

- **Create and elucidate clear processes for enforcement of laws regulating platforms, including how penalties should be determined and ensure these penalties accrue to the appropriately responsible party**. Policymakers should provide courts, platforms, and other relevant stakeholders with as much clarity and guidance as possible to ensure that the laws operate equally and do not inspire confusion in enforcement that may negatively impact human rights.

***Governments should require platforms to:***

- **Create systems to ensure transparency of their decision-making processes around content, including the impact of algorithmic decision-making and ranking on how users receive information.** It is not responsible for companies to operate technologies that are not subject to human governance and oversight. Ensuring that platforms' technical underpinnings are explainable, and potentially auditable, is necessary to promote accountability.

- **Ensure that there is transparency around rules and rights for users. Platforms should provide clarity for users about both their moderation rules and the rights users have for appeal or redress.** These should be both readily available in a range of languages, and clearly understandable for the average user.

- **Enable access to data for regulators and other public interest stakeholders in order to assess the platform's systems independently.** Policymakers can work with internet communications companies to establish privacy-preserving, secure data exchanges and facilitate access to social media data for regulators––and also for journalists, researchers, and non-governmental organizations, where appropriate––to enable thorough investigations and preservation of historically-important data, as well as auditability of the platforms' performance against their public commitments.

- **Create clear processes of appeal and redress around content decisions.** Platforms should provide users with mechanisms for understanding and appealing decisions to remove content or deactivate accounts.

## DIVING DEEPER

*Freedom and Accountability: A Transatlantic Framework for Moderating Speech Online*, Transatlantic Working Group

*Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*, Broadband Commission for Sustainable Development

*The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship*, Jacob Mchangama and Joelle Fiss

# AUTHORS


**Megan Metzger** is a Research Scholar and Associate Director of Research for the Global Digital Policy Incubator. She completed a PhD in Politics at NYU as a member of the Social Media and Political Participation Lab and her research focuses on how technology impacts rights and political behavior.

**Tracy Navichoque** is the Program Manager at the Global Digital Policy Incubator. She holds an MA in Public Diplomacy from USC and BA in History and International Studies from Northwestern University.

**Kip Wainscott** is a Senior Advisor for the Global Digital Policy Incubator. A lawyer and policy professional with experience in government, civil society, and the private sector, he has worked extensively on issues concerning technology's impact on democracy and human rights.

*With research assistance from Catherine Baron and Rosanna Kim.



**This snapshot was created in partnership with the International Center for Not-for-Profit Law.**