

Understanding the Splinternet and Addressing the Business Concerns it Poses

By *Jishnu Sanyal (Counsel)* and *Akanksha Bisen (Senior Manager)*

One of the rights guaranteed under the Universal Declaration of Human Rights, 1948¹ is the right to seek, receive and impart information and ideas through any media and regardless of frontiers. However, the rise of nationalism and protectionism globally is leading to the internet splintering into smaller parts, each of which is governed differently and therefore referred to as the splinternet. Instead of a single global internet, this would lead to multiple national or regional networks that do not speak to each other or possibly even are unable to due to incompatible technologies. Concerns around the splinternet include fragmented online marketplace (making it harder for companies to reach their target audiences) and the evolution of different business and compliance standards around data management, protection, and transactions. This presents new risks and compliance challenges for companies operating in multiple countries.

A good starting point for addressing potential risks and compliance concerns is understanding the evolution of internet regulation.

The free flow of data defined the early internet. However, eventually, jurisdictions started blocking certain sites, apps, and products due to their nature of work, content hosting, or simply because they originated from a hostile nation. Businesses no longer have unfettered access to the information, and Governments are increasingly restricting online content and apps. Most recently, we have seen Russia and various western nations block each other's content from being made available within their national boundaries². The calls for Russian domains to be revoked altogether, which would have effectively taken Russia off the internet, were also made to ICANN (Internet Corporation for Assigned Names and Numbers), albeit unsuccessfully³.

However, there has also generally been a rise in internet regulation globally across jurisdictions, especially concerning cross-border digital transactions, which has led to measures such as data localisation mandates. Consequently, Governments are effectively restoring the role of national borders in the digital economy.

Over 71% of jurisdictions have data privacy legislation, and another 9% are in the process of drafting one. In many countries, these legislations also govern their citizens' data privacy. These laws can increase market entry costs for foreign businesses, making it counterproductive for business investments as the mounting compliance costs may override expected profits. Specifically, in the case of new businesses such as digital assets, the splinternet may impact how these assets are taxed, resulting in an uneven playing field for businesses and increased compliance costs for foreign entities. Further, many businesses also tend to rely upon centralised global data centres, which may particularly impact such businesses.



Source: <<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>>

Therefore, it is essential for businesses dealing with data across multiple regions to actively start thinking about how these upcoming trends of internet regulation may hit their operations.

Managing your operations in the splinternet era

To ascertain the risks from the splinternet to your operations, businesses should consider the following questions:

1. Does the business have an international data strategy?
2. Does the business have a streamlined process and periodic assessments to respond to global regulatory changes?
3. Does the business effectively manage data processing and storage for data related to subjects based in the EU, China, Russia and other regions which have strong regulatory policies?
4. Does the business have a position and process to respond to local law enforcement data requests, including requests regarding content moderation?

While most businesses would have a constantly evolving position on these issues, it is important to consistently and periodically take stock and assess the businesses' international compliance and operations plan.

While businesses strive for global standards, they must consider the unique legal and compliance needs of the countries they operate in. Below are some suggestions to consider:

- (a) **Proactive audits:** Undertake audits across key relevant geographies to assess the legal landscape and the ongoing compliance and risks.
- (b) **Expert legal advice:** Ensure the organisation has access to experienced legal and compliance professionals in all geographies of interest who can help navigate the complexities of the law and suggest compliant business solutions.
- (c) **Assess business models:** Be prepared to revisit business models and the supporting processes such as data collection, storage, and monetisation. This can pose particular challenges for single product/ service companies that sell on a licence basis or for businesses that are volumes driven.
- (d) **Consider the cost of legal due diligence and ongoing compliance:** This can be done at the market entry planning stage, including market research on the current legal landscape and estimation of ongoing compliance costs.
- (e) **Set up local infrastructure and ops to comply with regulations:** While this may dent the unique selling proposition of some enterprises as “operate-from-anywhere-businesses”, it can ensure sustenance of operations.
- (f) **Develop a robust risk management strategy:** Appoint a dedicated compliance officer depending on the company's size and scope of its operations.
- (g) **Establish clear communication channels:** Effective communication between various business units is vital for awareness of and compliance with the latest regulations. MNCs, specifically, should monitor their compliance programs on an ongoing basis and leverage digital tools to aid this.
- (h) **Access to an ecosystem of disputes lawyers:** Content/data laws can be conflicting depending on the jurisdiction of residence and where the online activity took place. Furthermore, countries

have conflicting opinions on the ambit of these regulations to restrict freedom of speech or data privacy. As internet laws continue to evolve, a rise in disputes over their interpretation is likely. Therefore, building an in-house disputes team or gaining access to external counsels may nip these issues in the bud.

Conclusion

Dealing with the splinternet requires organisations to have a flexible and adaptable business strategy. It is important for businesses to continuously evaluate their positions and undertake the various measures outlined to ensure compliance and avoid disputes that may threaten the business itself. While businesses may not be in a position to effectively respond to widespread content takedown based on purely national interests such as the ones related to the Russia-Ukraine situation, they must adapt to regulatory changes regarding data protection, localisation and content regulations, which will only continue to see widespread adoption across more nations.