CENTER for NEWS, TECHNOLOGY & INNOVATION.
Using global research & collaboration to promote an informed digital society.

innovating.news

Open Distribution & Access

Protecting an Open Internet

How can we discourage the development of 'splinternets' and encourage the protection of an open internet?

CNTI's Assessment

An open internet infrastructure is critical to functioning, free societies. As governments around the world increasingly turn their attention to issues of internet governance — including via efforts to tackle disinformation and protect user data — the risk of "splintered" internet experiences grows. Policy frameworks should adress the distinctions among different forms of fragmentation, the (limited) scenarios in which content fragmentation is justified and how to minimize the impact of fragmentation. Internet regulation that discourages the "splitnernet" distributes power outside of the government, protects and promotes individual rights (regarding encrypted and personal data) and open and transparent standards, and accounts for the global nature of the internet — particularly when it comes to the rights of journalists and citizens to communicate and share information within and across borders. Support for independent online media is critical to the protection of an open, globally connected internet.

	Open Internet	Splinternet
Facebook	✅	❌ Blocked
Wikipedia (English Version)	✅	! Something that looks like English Wikipedia but is in a different language—and may or may not actually be Wikipedia
Google	✅	! Different search engine, displaying only government-approved sources.

Source: Internet Society

The Issue

The internet, as a public good, can provide access to reliable and independent news as well as exposure to diverse sources and perspectives. But amid changing geopolitical contexts, new technologies and the threat of online abuse and disinformation, policymakers around the world are increasingly leading governments into rethinking models of internet governance.

These political, commercial and technological pressures risk splintering the internet into a collection of different networks and user experiences based on one's location in the world (also referred to as "fragmentation" or "balkanization"). In fact, splintering is already occurring in some places; two users may encounter wholly different internet experiences based solely on their location. While practices that result in splintering are often enacted by autocratic regimes – via rhetoric, technological developments and legislation – these types of practices are also increasingly central to internet policy debates in democratic societies.

In weighing the challenges of this issue, it is helpful to distinguish between two types of systems: those where a "splinternet" is intentionally sought out, often to assert state control over data and digital assets or to cut off public access to independent information, and those where a "splinternet" is an unanticipated byproduct of governments' (or even corporations') attempts to prevent the spread of disinformation, address legitimate online harms and/or protect citizens' data from foreign interference.

There are crucial differences between these two systems, but both introduce risks if they do not include safeguards that protect both user rights and a free flow of global information.

The challenge is to ensure that the public's ability to use the internet to create, share and access information as well as journalists' ability to report and distribute it is protected – both within and across borders.

Find the full issue primer, current legislation, events, and changemakers online
https://go.innovating.news/0PglE8

What Makes It Complex

I. Internet "fragmentation" does not have a singular definition, so policies responding to the risks associated with fragmentation must be tailored to the particular context.

II. Policymakers tasked with assessing or rethinking models of internet governance face challenges in foreseeing unintended consequences of policies if they don't have access to technical expertise in the nuances of how the internet works.

III. Bans on specific digital platforms have become a common response to concerns about online safety and disinformation, but they increase the risk of internet fragmentation, threaten free expression and can encourage copycat legislation.

IV. The 'splinternet' presents new challenges for corporations asked to comply with demands that would permit governments' abuse of power.

V. Protecting an open internet is not always possible in autocratic societies, but actions taken elsewhere can still have global impact.

VI. It is crucial to consider the impact of zero rating programs on an open internet.

VII. The contemporary internet is still not a truly universal or open network; access and language translation vary considerably around the world.

Notable studies

Splintered speech: Digital sovereignty and the future of the internet - PEN America (2021)

Summary: This 2021 report draws upon expert interviews and literature reviews to identify different conceptions of digital sovereignty, summarize developments in the U.S.and offer recommendations for digital regulation that protect international human rights.
CNTI's Takeaway: Policy frameworks should consider this report's recommendations to center human rights in digital regulation such as adopting human rights impact assessments for all proposed legislation and executive action.

State of Research

A growing segment of public-facing research conducted by independent research institutions, open internet advocacy organizations and (inter)governmental bodies (several of which we note in this primer) has focused specifically on assessing the increasing threat of the "splinternet."

As platform bans become a more commonly discussed approach to addressing online safety and disinformation, research analyzing the scope and impact of these policy debates will be particularly useful. This includes how particular policy language is adopted in one context and readopted elsewhere over time and on a global scale.

State of Legislation

Internet governance represents a broad range of stakeholders and mechanisms, including national and international legislative policy as well as technological design, company policies and global regulatory institutions.

In some cases, legislation attempts to protect societies from a "splinternet." In others, legislation risks encouraging a "splinternet" either intentionally or unintentionally.

Legislative efforts that protect an open internet should consult resources and recommendations provided by global internet experts. These include ensuring that governments can only collect or access online user data for transparent and legitimate purposes, promoting open standards among new technologies and platforms, protecting encryption, maintaining access to internet services and digital platforms, supporting independent online media and addressing the digital divide.

Notable legislation

India: India's government has expanded digital censorship efforts since 2019 through legislation, internet shutdowns, platform bans and heightened scrutiny of platforms. In 2021, an executive order introduced internet regulations which forcetechnology companies to comply with government surveillance and undermine user rights. It targets end-to-end encryption protocols, requiring messaging apps to trace and reveal senders' identities. This threatens free expression and an open internet.

CNTI

The Center for News, Technology & Innovation (CNTI), an independent global policy research center, seeks to encourage independent, sustainable media, maintain an open internet and foster informed public policy conversations.