

Protecting an Open Internet

How can we encourage the protection of an open internet?



CENTER for NEWS,
TECHNOLOGY & INNOVATION.

CNTI's Assessment

An open internet is essential to free societies, but as governments worldwide turn their attention to internet governance — from disinformation to data protection — the risk of a fragmented online experience is growing. Some fragmentation is deliberate, often used by states to assert control over data or limit access to independent information. Much of it, however, is the unintended consequence of well-meaning policies that fail to account for the internet's inherently global nature.

Sound regulation should distinguish between these forms and pursue intermediate goals that protect openness: distributing power beyond governments, discouraging corporate consolidation, protecting individual and encrypted data rights, and promoting open standards that don't lock users or publishers into specific platforms. Policy frameworks should also account for the global flow of information, particularly the rights of journalists and the public to communicate and share across borders.

The stakes are particularly high for journalism. Internet blocks and shutdowns make it harder for news providers to report and distribute their work, and they limit the public's access to information beyond what governments allow — a sharp concern for online-only and online-first outlets, which often surface the censorship threatening an open internet in the first place. Tech stakeholders share responsibility too: building encryption in by default, participating in multistakeholder governance and supporting interoperable standards are practical levers for keeping the internet open and genuinely useful across borders.

The Issue

The global internet was once seen as a force for free and open societies — a digital civic space that could transcend borders and connect people to diverse, independent information. But amid shifting geopolitics, new technologies and growing threats from [online abuse](#) and [disinformation](#), policymakers worldwide are rethinking how the internet is governed. At the heart of these debates is a fundamental question: who controls how the global internet functions, and on what terms?

The risk is [fragmentation](#) — the splintering of a once-unified internet into a patchwork of disconnected networks and user experiences, often shaped by where someone lives or which company connects them. Sometimes called the “splinternet,” this fragmentation is already underway. While it's most often associated with [autocratic regimes](#) that censor or wall off the internet to suppress independent information, it is increasingly shaping policy debates in [democracies](#) as well, through content takedowns, platform blocks, network shutdowns and other regulatory tactics.

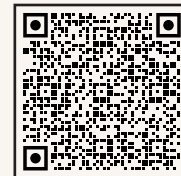
It's useful to distinguish two paths to fragmentation: deliberate efforts by governments to assert control over data and limit access to [independent information](#), and unintended consequences of well-meaning policies aimed at [curbing disinformation](#), addressing online harms or protecting residents' data. Both carry risks without safeguards for user rights and the free flow of global information. The stakes are particularly high for journalism, which depends on open digital channels to report and distribute news — especially when platforms are infiltrated or blocked by the state. Watchdogs report that online censorship and manipulation are growing worldwide, threatening press freedom, journalist safety and public access to information.

As governments weigh approaches to internet regulation, they should recognize that some responses risk fragmenting the internet while others protect against it. At its most harmful, fragmentation entrenches government and corporate power in ways that erode free expression and privacy. The challenge is ensuring policy preserves the public's ability to create, share and access information across borders — and journalists' ability to do the same.

	Open Internet	Splinternet
Facebook	✓	✗ Blocked
Wikipedia (English Version)	✓	! Something that <i>looks</i> 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](#)

FULL ISSUE PRIMER



Protecting an Open Internet

How can we encourage the protection of an open internet?

What Makes This Complex

- I. Internet fragmentation does not have a singular definition. As a result, it is hard to identify and address risks with comprehensive policy.
- II. 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 and, some argue, threaten free expression.
- III. There is legitimate disagreement about the bounds of free speech, even among democratic societies.
- IV. Internet fragmentation 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 still impact people living under these autocratic regimes.
- VI. Consolidation of infrastructure among a few large companies may counterbalance state power — but it increases other risks.
- VII. Zero-rating programs can prevent people from accessing the complete, open internet.
- VIII. The contemporary internet is still not a truly universal or open network; technical and linguistic access vary considerably around the world.
- IX. Policymakers may not have access to nuanced technical expertise in how the internet works, which can make it harder to foresee unintended consequences.

Notable studies

Internet Fragmentation's Outward Turn - Maily Fidler - Harvard National Security Journal - 2026

Summary: While many scholars analyze internet fragmentation as primarily domestic, this analysis pivots to outward-facing developments. It lays out a recent shift from protectionism to fragmentation through actions like export controls, undersea cable sabotage, selective infrastructure investment and fragmented legal regulation.

CNTI's takeaway: As internet fragmentation "is now deployed to subvert the interests of other states," governance questions grow more complex. Beyond limiting their own populations' access, "outward facing" fragmentation may risk escalating armed conflict, which other studies link to internet shutdowns and censorship.

State of Research

To date, much of the work on internet governance has centered on "digital authoritarianism" (particularly China and Russia) and the European Union's digital sovereignty agenda. A growing body of research is beginning to assess internet fragmentation more broadly, but most offers case studies or narrow policy analysis — and a lack of consensus on what "freedom" and "censorship" entail complicates agreement on interventions.

As platform bans, data localization and age verification gain traction in debates over online safety and disinformation, systematic research on the scope and impact of these policies — and how their language travels across borders — will be especially valuable elsewhere over time and on a global scale.

State of Legislation

The internet is now a central locus of global policymaking as governments debate how to regulate digital spaces within (and sometimes outside) their own borders. Internet governance spans national and international policy, infrastructures, technical standards and company policies, with a recent shift toward "digital sovereignty" — governmental capacity to control residents' content and data flows. Some legislation seeks to protect societies from a fragmented internet; other measures risk encouraging fragmentation through closed national intranets, platform blocks or online governance laws with indirect consequences for free expression.

Those developing legislation to protect an open internet should consult resources and recommendations from global experts: limiting government access to user data, protecting encryption and VPN access, building interoperable privacy regimes, and maintaining access to services and platforms.



Notable legislation

China: Supported by legislation, China's "Great Firewall" is a sophisticated surveillance and blocking system that prevents Chinese citizens from accessing foreign information sources, internet tools and mobile apps. Some provinces have implemented additional, even stricter censorship. In 2025, China developed ships capable of cutting undersea fiber-optic cables, enabling them to interfere in other countries' internet access.