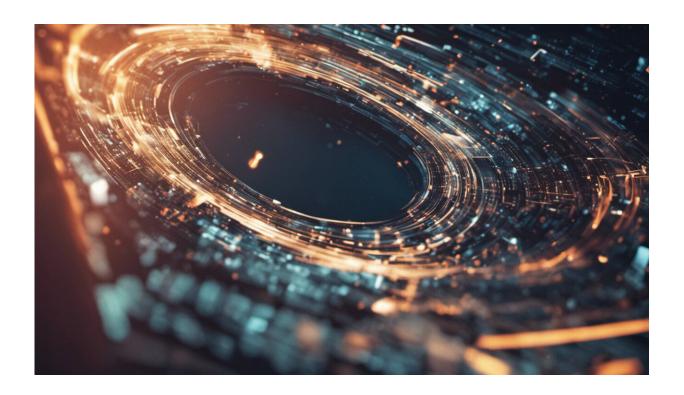# What is the 'splinternet'? Here's why the internet is less whole than you might think

June 9 2023, by Robbie Fordyce

Credit: AI-generated image ([disclaimer](#))

"Splinternet" refers to the way the internet is being splintered—broken up, divided, separated, locked down, boxed up, or otherwise segmented.

Whether for nation states or corporations, there's money and control to be had by influencing what information people can access and share, as

well as the costs that are paid for this access.

The idea of a splinternet isn't new, nor is the problem. But recent developments are likely to enhance segmentation, and have brought it back into new light.

The internet as a whole

The core question is whether we have just one single internet for everyone, or whether we have many.

Think of how we refer to things like the sky, the sea, or the economy. Despite these conceptually being singular things, we're often only seeing a perspective: a part of the whole that isn't complete, but we still experience directly. This applies to the internet, too.

A large portion of the internet is what's known as the "[deep web](#)". These are the parts search engines and web crawlers generally don't go to. Estimates vary, but a rule of thumb is that approximately 70% of the web is "deep".

Despite the name and the anxious news reporting in some sectors, the deep web is mostly benign. It refers to the parts of the web to which access is restricted in some ways.

Your personal email is a part of the deep web—no matter how bad your password might be, it requires authorization to access. So do your Dropbox, OneDrive, or Google Drive accounts. If your work or school has its own servers, these are part of the deep web—they're connected, but not publicly accessible by default (we hope).

We can expand this to things like the experience of multiplayer videogames, most social media platforms, and much more. Yes, there

are parts that live up to the ominous name, but most of the deep web is just the stuff that needs password access.

The internet changes, too—connections go live, cables get broken or satellites fail, people bring their new Internet of Things devices (like "smart" fridges and doorbells) online, or accidentally open their computer ports to the net.

But because such a huge portion of the web is shaped by our individual access, we all have our own perspectives on what it's like to use the internet. Just like standing under "the sky", our local experience is different to that of others. No one can see the full picture.

A fractured internet poised to fracture even more

Was there ever a single "Internet"? Certainly the US research computer network called [ARPANET](#) in the 1960s was clear, discrete, and unfractured.

Alongside this, in the '60s and '70s, governments in the Soviet Union and Chile also each worked on similar network projects called [OGAS](#) and [CyberSyn](#), respectively. These systems were proto-internets that could have expanded significantly, and had themes that resonate today—OGAS was heavily surveilled by the KGB, and CyberSyn was a social experiment destroyed during a far-right coup.

Each was very clearly separate, each was a fractured computer network that relied on [government support](#) to succeed, and ARPANET was the only one to succeed due to its significant government funding. It was the kernel that would become the basis of the internet, and it was [Tim Berners-Lee's work on HTML at CERN](#) that became the basis of the web we have today, and something he seeks to protect.

Today, we can see the unified "Internet" has given way to a fractured internet—one poised to fracture even more.

Many nations effectively have their own internets already. These are still technically connected to the rest of the internet, but are subject to such distinct policies, regulations and costs that they are distinctly different for the users.

For example, Russia maintains a Soviet-era-style surveillance of the internet, and is far from alone in doing so—thanks to Xi Jinping, there is now "the great firewall of China".

Surveillance isn't the only barrier to internet use, with harassment, abuse, censorship, taxation and pricing of access, and similar internet controls being a major issue across many countries.

Content controls aren't bad in themselves—it's easy to think of content that most people would prefer didn't exist. Nonetheless, these national regulations lead to a splintering of internet experience depending on which country you're in.

Indeed, every single country has local factors that shape the internet experience, from language to law, from culture to censorship.

While this can be overcome by tools such as VPNs (virtual private networks) or shifting to blockchain networks, in practice these are individual solutions that only a small percentage of people use, and don't represent a stable solution.

We're already on the splinternet

In short, it doesn't fix it for those who aren't technically savvy and it doesn't fix the issues with commercial services. Even without censorious

governments, the problems remain. In 2021, Facebook shut down Australian news content as a protest against the News Media Bargaining Code, leading to potential change in the industry.

Before that, organizations such as Wikipedia and Google protested the winding back of network neutrality provisions in the US in 2017 following earlier campaigns.

Facebook (now known as Meta) attempted to create a walled garden internet in India called Free Basics—this led to a massive outcry about corporate control in late 2015 and early 2016. Today, Meta's breaches of EU law are placing its business model at risk in the territory.

This broad shift has been described in the past by my colleague Mark Andrejevic in 2007 as digital enclosure—where states and commercial interests increasingly segment, separate and restrict what is accessible on the internet.

The uneven overlapping of national regulations and economies will interact oddly with digital services that cut across multiple borders. Further reductions in network neutrality will open the doors to restrictive internet service provider deals, price-based discrimination, and lock-in contracts with content providers.

The existing diversity of experience on the internet will see users' experiences and access continue to diverge. As internet-based companies increasingly rely on exclusive access to users for tracking and advertising, as services and ISPs overcome falling revenue with lock-in agreements, and as government policies change, we'll see the splintering continue.

The splinternet isn't that different from what we already have. But it does represent an internet that's even less global, less deliberative, less

fair and less unified than we have today.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation