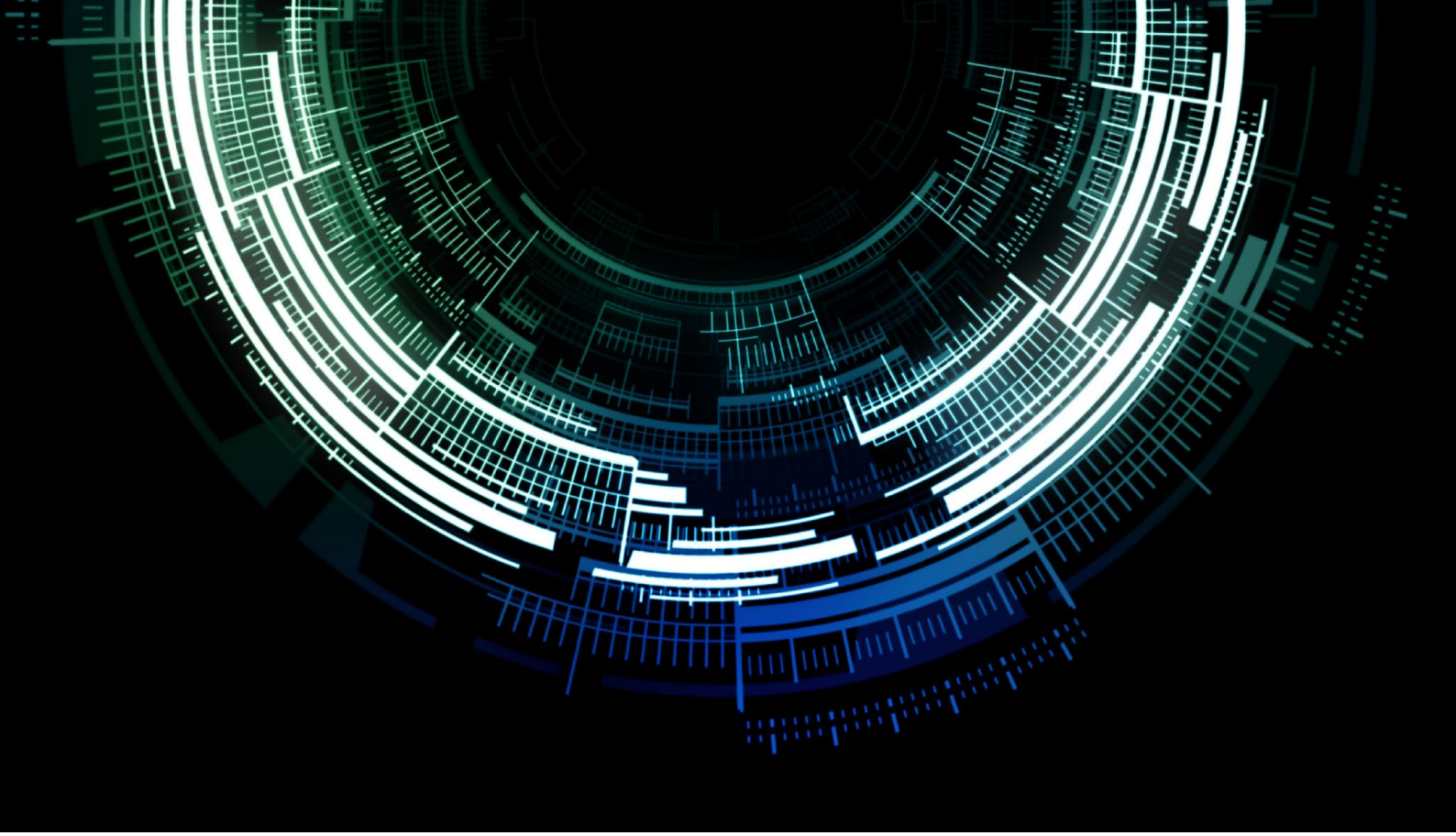

Steve Song

Internet Drift: How the Internet is Likely to Splinter and Fracture

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Steve Song

Internet Drift: How the Internet is Likely to Splinter and Fracture

The idea of a "splinternet" or "Balkanization" of the internet is not new, although the exact manner by which this is becoming a reality is evolving. Early discussions on the topic focused around cultural or policy differences and extraterritoriality that could result in a **fractioned internet**. For example, China's Great Firewall is implementation of a national policy which creates an "intranet" connected to the greater Internet.

However, there is another shift in internet infrastructure that is less talked of and even more fundamental to its functioning – the physical backbone of fibre optic cables crossing oceans and international borders that enables the relatively seamless experience of the Internet regardless of location. Increasingly investment and ultimately ownership and control of the cables used to transport information across the world is moving away from telecommunications operators. One example is the increased investment in and ownership of trans-oceanic cables by application and service providers, or platforms, such as **Google, Facebook, and Microsoft**. Another is the strategic investment in undersea cables by nation states as part of a geo-political cyber strategy.

Internet Giants and Undersea Cables

Historically, undersea cables were either publicly owned or owned and operated by telecommunications network operators (telcos) which had little to do with content or application delivery, unlike digital platforms like Google, Facebook and others that are now beginning to expand their private networks. The demand for global, high-speed, low-latency services has driven the development of local data centres which can serve a platform's content instantly almost anywhere in the world. Keeping these local data centres up-to-date consumes six to seven times more **undersea traffic** than the rest of the public internet combined.

Not surprisingly, platforms have begun to invest in the Internet's long-distance transport layer, such as undersea cable capacity, in order to serve these networks of data centres – also largely owned and operated by the platforms themselves. In contrast, what is called "last mile" of content delivery (moving content from the data centre to the end user) is still largely owned and operated by telcos. What began as investment in data capacity on existing cables rapidly became investment in the undersea cables themselves, many of which are now either partly or wholly-owned by content platform companies. The implications of this are sobering.

An undersea cable owned by a platform such as Google, Facebook or Microsoft becomes a private network connecting their data centres. As such, these cables are not governed according to the rules that have governed the Internet and its network operators to date, those of common carriage and neutrality. The telco industry, having a long history dating back to the telegraph, has had a fairly standard regulatory structure with a strict delineation between content providers (e.g. a phone company or Google) and the non-discriminatory network infrastructure which carries communications. Companies like Google are keen to avoid regulation and, as a result, have **publicly stated** that they will not resell capacity on their cables because they would then effectively operating as a telco and be subject to the oversight of telecommunications regulation.

However, this would not prevent platforms from engaging in capacity swaps with other platforms that own capacity with the result that a significant percentage of international internet traffic will not be subject to any regulatory framework. It may also result in a closed club of undersea capacity that is only accessible to other data platforms with similar investments.

Worse, because platforms account for so much international traffic, their decision to invest in their own undersea cables is likely to have a significant negative impact on investment and growth of undersea cables not owned by platform companies.

This is likely to have the effect of consolidating the dominance of a few large platform companies that can offer performance through their private networks that eclipse the public internet. Net neutrality regulations will not have any power to influence this shift.

> What began as investment in data capacity on existing cables rapidly became investment in the undersea cables themselves, many of which are now either partly or wholly-owned by content platform companies. The implications of this are sobering.

State Dominance of Infrastructure

Nation states, most notably China, are pursuing strategies that are not dissimilar to the Silicon Valley platforms. China is investing a significant amount of resources to build a geographically strategic infrastructure making it possible for internet data to flow around the world entirely on fibre optic infrastructure owned by China. The **SAIL cable** linking Africa with South America, the **PEACE cable** linking Asia to Africa, as well as a possible **Trans-Pacific initiative** linking China directly to South America are all examples of this. Growth in China's outward expansion and investment in communications infrastructure development geographically overlaps with many of the initiatives in its **Belt and Road Strategy**, which seeks to strengthen China's economic ties with 71 countries (accounting for over half the world's population) through investment in roads and waterways – and the building of Internet infrastructure mirrors these areas of investment.

The focus of development of this infrastructure may be between governments or regions that share governance structures and ideologies – particularly authoritarian regimes. This may reduce people's access to information, association and participation in online forums. New communication technologies in this vein may further infringe on digital rights such as privacy and freedom of expression by **embedding surveillance** or even censorship capabilities in the

infrastructure that would be in the hands of governments. At a higher level, these expansive policies and strategies are already impacting **democracy and national sovereignty.**

Conclusion

For consumers, this shift to a less public internet – whether by big tech giants or nation states – would limit enforcement of digital rights. What can digital rights defenders do? Digital rights defenders should engage with standards development organisations – such as IETF, regional standards bodies, or even join a member state's delegation at the ITU – and other open internet governance processes to support an open internet model. They should also engage directly with governments to build a mutual support for and understanding of the benefits of an open internet, and the internal costs of adopting more restrictive technologies and building redundant infrastructure. Particular attention should be paid to landing stations and the terms on which undersea cables are granted landing rights.

Rights defenders should also build awareness and understanding of the impact of both privatisation and splintering of the internet so that they may urge their governments and policymakers to take appropriate steps. One such approach might be to consider the use of anti-trust laws to break up media conglomerates, particularly those found to be in violation of local laws or deemed "outside" regulation due to their strategically built ecosystem. Likewise, national regulatory bodies or other organisations may be able to use litigation based on existing laws such as competition, consumer rights, and data protection to pressure platforms to act in a manner that supports a free and open Internet and robust marketplace.

Rights defenders should also build awareness and understanding of the impact of both privatisation and splintering of the internet so that they may urge their governments and policymakers to take appropriate steps.

About Steve Song

Steve Song is a Mozilla Fellow and research associate with the Network Startup Resource Center (NSRC). He writes at www.manypossibilities.net

---

Internet Drift: How the Internet is Likely to Splinter and Fracture

Future-Proofing our Digital Rights

About the Digital Freedom Fund

The **Digital Freedom Fund** supports strategic litigation to advance digital rights in Europe. With a view to enabling people to exercise their human rights in digital and networked spaces, **DFF** provides financial support for strategic cases, seeks to catalyse collaboration between digital rights activists, and supports capacity building of digital rights litigators. **DFF** also helps connect litigators with pro bono support for their litigation projects. To read more about DFF's work, visit: **www.digitalfreedomfund.org.**

The **Future-Proofing Our Digital Rights** project was made possible thanks to the support of the Foundation for Democracy and Media and the Renewable Freedom Foundation. **DFF** receives organisational support from Open Society Foundations, Luminate and Adessium Foundation.

Democracy & Media Foundation **Stichting Democratie & Media**

Renewable Freedom Foundation

DFF Digital Freedom Fund

E-mail:
info@digitalfreedomfund.org

Postal address
Digital Freedom Fund
P.O. Box 58052
1040 HB Amsterdam
The Netherlands