Internet Way of Networking Use Case

Intermediary Liability

September 2020

Intermediary liability protection and the Internet Way of Networking

What is intermediary liability protection?

There are several actors along the path that a message - whether an email, cat video, voice call, or web page - travels on the Internet. Each one of them might be considered an "intermediary" in the transmission of the message.

Examples of Internet infrastructure intermediaries include Content Delivery Networks (CDNs), domain name registries, and registrars. They manage network infrastructure, provide access to users, and ensure delivery of content. These mostly private sector companies provide investment and upkeep of the services we all use.

Unlike broadcasting, where the carrier also controls the content, an intermediary delivering infrastructure services, such as an Internet service provider (ISP), is unlikely to be aware of the content of the message they are carrying. These entities merely relay packets on the Internet to other destinations. Even if they are theoretically able to inspect the content of those packets – which is increasingly impossible due to encryption – they do not produce the content. Like postal and telephone services, they have the essential role of carrying the underlying message efficiently.

Intermediary liability protection was formalized around the world to allow intermediaries to focus on developing their business models and securing investment without fear of being held responsible for data that passed through their network. As long as intermediaries are responsive to requests to remove illegal content, they are not legally or financially liable for the content of the data they transmit or host.

The United States' 1996 Communications Decency Act, Section 230, its 1998 Digital Millennium Copyright Act, Section 512, and the European Union's 2000 E-Commerce Directive each enshrined the protection of Internet intermediaries from liability for the actions of their users.

These and many similar laws around the world treat Internet intermediaries not as publishers of content, but as a conduit for data and information published by users of the services.

The following provides an overview of how increasing attempts to revisit existing intermediary liability regimes can threaten the original intention of laws aligned with the critical properties that have made the success of the Internet possible. It also explains why an indiscriminate overhaul of the intermediary liability regime, without the

close considerations of different roles and functionalities afforded in the original thinking behind these laws, is likely to harm the Internet Way of Networking in the future.

Current trends

In recent years, there have been a growing number of dangerous attempts in different countries to revise long-standing intermediary liability protection regimes. The current focus is on intermediaries offering services 'higher up' the Internet stack, on platforms such as Facebook, Twitter, and Amazon. Policymakers are re-considering the role of intermediaries in disseminating disinformation, or whether messaging services should use end-to-end encryption. Policymakers in Europe and the US are also reviewing what constitutes an intermediary in this context. At the same time, there is an emerging trend among the law enforcement community in various countries expecting infrastructure providers far down the Internet's layers to police content that users see. For example, in 2019, an Italian Court ordered the CDN and Distributed Denial of Service (DDoS) protection services company, Cloudflare, to terminate the accounts of a number of contested pirate sites. In addition, Cloudflare was ordered to share the account details and their hosting companies with the complainant, RTI.[1]

If this trend continues, infrastructure providers such as network operators may be seen as liable for the data they pass across their networks and could therefore be forced to implement technical measures to check and remove content. Content-blocking measures by operators include IP and protocol-based blocking, deep packet inspection (i.e. viewing content of "packets" as they move across the network), and URL and DNS-based blocking.[2]

These measures 'over-block', imposing collateral damage on legal content and communications. They also interfere with the functioning of critical Internet systems, including the DNS, and compromise Internet security, integrity, and performance.

The wide range of Internet infrastructure intermediaries – from ISPs to CDNs supporting gaming and video, to domain name system registries and registrars, and more – mean that removing liability protections has profound and unpredictable negative consequences throughout the infrastructure of the Internet. It could put intermediaries in an impossible situation where instituting the changes necessary to reduce their liability makes it impossible to continue providing a service.

Furthermore, given the global nature of Internet traffic flows, many infrastructure intermediaries could be required to implement the competing policies and laws of different countries – an impossible promise to keep.

If policymakers remove the key protection that has allowed these infrastructure intermediaries to operate and innovate, they will be less able to perform their core functions and attract necessary investments, and the Internet as we know it will be severely damaged.

Which critical properties does intermediary liability protection impact?

Critical Property 2 – An Open Architecture of Interoperable and Reusable Building Blocks

The Internet is made up of re-usable building blocks – technologies and protocols assembled in an open architecture. These building blocks are assembled and used in different ways by different intermediaries that play various roles in the value chain and who have a wide variation of relationships to data and knowledge of its content.

1 https://torrentfreak.com/court-orders-cloudflare-to-terminate-accounts-of-pirate-sites-190711/

2 The Internet Society's 2017 policy paper on Internet Content-Blocking describes in more detail these methods and their impacts on the Internet, including URL (universal resource locator) and DNS (domain name system) methods of blocking: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

For example, while a network operator or a CDN might simply ensure that data is moved to the proper destination, an application provider is responsible for knowing the meaning and value of the data. To this end, the primary responsibility of infrastructure intermediaries is to participate in the transfer of data, rather than knowing the content of that data. Because of this complexity, attempts to impose intermediary liability indiscriminately could over-simplify the complex and varying roles different intermediaries play, and assume they have more real-time knowledge of the content of data that crosses their networks. In reality, in today's Internet, intermediaries are extremely diverse and perform such a wide variety of different functions that a one-size-fits-all approach is not advisable.

The current intermediary liability regime recognizes the importance of the end-to-end principle – the idea that intelligence in the network resides at the ends or in the applications, leaving the function of the network itself relatively simple. In a nutshell, intermediary liability protection acknowledges that infrastructure providers (such as ISPs, CDNs, or DNS providers) play a different role than the services (such as websites) that publish content in the application layer above them.

A change in the regime could affect interoperability of the building blocks and applications across networks, undermining the so-called end-to-end principle where the networks are agnostic to the data they pass along. This would make innovation more difficult, since applications would need to consider additional network functionality, or make complex arrangements with the network.

Critical Property 3 - Decentralized Management and Distributed Routing

The Internet is a 'network of networks', made up of almost 70,000 independent networks that use the same technical protocols and choose to collaborate and connect together. Each network makes independent decisions on how to route traffic to its neighbours, based on its own needs, business model, and local requirements. There is no centralized control or coordination. The ability to make independent decisions about how to route traffic allows each part of the Internet to quickly adapt to operational requirements and the needs of users.

Reducing liability protection would force infrastructure intermediaries to impose additional requirements on routing policy that conflict with the current goals of maximizing resilience, reducing costs, and optimizing traffic flows. This would reduce network operators' routing autonomy and their ability to optimize connectivity.

Inevitably, different countries would have different liability rules. Internet traffic may pass through a jurisdiction with weakened liability protection. Policymakers usually focus on content in a single jurisdiction, but the Internet works to route traffic in the most efficient way possible, often travelling through multiple jurisdictions. Presented with a requirement to ensure certain types of content do not enter a certain jurisdiction, an operator making best efforts may still be unable to comply. The network operator may try to make its traffic conform to the regime of countries the traffic may or may not route through, even if those requirements are different or much more rigid compared with those in the operator's and users' countries, or it may incorporate in its routing policy a rule never to route traffic to intermediaries in a specific jurisdiction. Even if these choices are available, an operator trying to ensure traffic satisfies the requirements of different jurisdictions with incommensurable liability regimes will be unable to comply with both.

All such efforts change network topology – the dynamically changing layout – of the Internet in fundamental ways that are at odds with routing efficiency and resilience, as they force the operator to try to align routing policy with the non-technical requirements of different jurisdictions.

Reduced liability protection interferes with the autonomous and agile distributed routing of the Internet, reduces the ability to collaborate with other networks, and ultimately constrains the Internet's global reach.

Critical Property 5 – A Technology Neutral, General-Purpose Network

The Internet is a 'technology neutral, general-purpose network' because there is no defined limit to the uses it can support. The intermediaries that make up the Internet serve a primary role: allowing their users to access the rest

of the Internet via their networks. There is no prior expectation that networks include points of control, and nor should there be.

A technology neutral, general-purpose network requires operators of network services to perform only basic functions, passing opaque data on to its next destination. Any additional requirements based on all operators understanding the nature of the data/content inevitably make a network more specialized and less general in its purpose. Imposing liability on infrastructure intermediaries would require them to take on additional roles that move them away from facilitating data transmission and more narrowly prescribe the functions of networks overall.

This would reduce the network's openness to new uses and new entrants, as well as affecting its speed and scale. Ultimately, this will damage the Internet's capacity to generate future innovation.

Conclusion

Protecting infrastructure providers from legal liability for how others use the networks made possible the investment in and building of a global Internet infrastructure and the explosion of innovative services that use it. At the same time, it has allowed for the development of transparent and proportionate public policy for law enforcement to require intermediaries to remove illegal content and communications. Intermediary liability protection helped make the Internet the global phenomenon it is today, and it underpins the investment and openness needed for the Internet to support future innovation.

Intermediary liability protection legally underpins three of the critical properties that make the Internet what it is: a technology neutral general-purpose network with open architecture, common services, decentralized management, and distributed routing. Its reduction or removal in specific countries will create operational impacts that harm the Internet as a whole. The increased cost and risk for operators and service providers will mean lower investment, diversion of limited resources to non-core activity, and a lessening of the effectiveness and value of the network as a whole.

Although there is a necessary policy conversation about the changing roles, scope, and responsibilities of some intermediaries, liability protection continues to be essential for infrastructure providers and any other actor participating in the "Internet Way of Networking".