Internet Way of Networking Use Case: Content Filtering

How content filtering impacts the Internet Way of Networking

This use case analyzes the effect that government policies requiring content filtering may have on the Internet Way of Networking. To understand how such policies could undermine the Internet's broader benefits such as innovation and socioeconomic growth we view them through the lens of the Internet's critical properties.

What is content filtering?

From foreign gambling websites in Europe and North America to political speech in China, the use of Internet content filtering techniques to prevent access to content considered illegal under national laws is a worldwide phenomenon. Content filtering (also called "content blocking") is a practice in which Internet users are denied access to certain online content based on government requirements. National authorities may enact public policies to restrict or prevent access to content such as child abuse material, content that violates intellectual property laws, threatens national security or is prohibited for a range of cultural or political reasons. Content filtering is legally and operationally complex; for example, content that is legal in one country may be forbidden in another.[1]

It is important to note that content filtering does not include measures implemented by network operators to manage their networks (traffic management)[2] or to counter network security threats (e.g. measures that address spam and malware). We also exclude processes to remove content using 'notice and takedown' processes aimed at potentially illegal content, and content moderation processes employed by, for example, technology platforms. Our focus is on technical measures that pre-emptively interfere with the movement of data that is not illegal, but may be unwanted for political or cultural reasons, as it travels through the Internet's infrastructure.

Content filtering interferes with the functioning of the Internet because some of its methods require the examination of traffic, including encrypted traffic, to determine its content. This practice is called Deep Packet Inspection (DPI). Other content filtering methods interfere with the operation of the Internet's global identifiers, including IP numbers and the Domain Name System (DNS). In DNS-based content filtering, when users type in a domain name, a server returns

1 A comprehensive analysis of content filtering is: "Internet Society Perspectives on Internet Content Blocking: An Overview", 2017 https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

2 "Policy Brief: Network Neutrality", https://www.internetsociety.org/policybriefs/networkneutrality/

incorrect information, either by sending the user to an IP address for a site with a notice saying the content is blocked, or simply saying the correct site does not exist.

At its most extreme, all traffic entering and leaving a country can be filtered for blocking at the national level. This requires tight control of all cross-border connections using a national gateway or firewall, as used in China,[3] Iran[4] and several Gulf states.[5] Filtering can also be imposed on network operators and other communication service providers (e.g. mobile operators and ISPs) who are required to install monitoring and blocking tools. Filtering and blocking can occur at many points between an Internet user and the content they wish to access or transmit, for example in their home, company or school network, local Internet service provider, the DNS resolver, hosting or cloud provider or via the search engine. To analyse the impacts of content filtering on the Internet Way of Networking, we focus here on network operator activities and filtering that uses the Internet's global identifiers (DNS and IP numbers).

What does content filtering mean for the Internet's critical properties, and what would happen if more countries imposed these restrictions?

Current trends

There is an emerging trend of significantly more aggressive, speedy and widespread use of content filtering and blocking by governments, as "digital authoritarianism sees governments taking control of Internet infrastructure, increasing online surveillance and controlling content."[6] Many governments around the world have required URL and DNS-blocking of content. For example, in 2019, a Turkish court named over one hundred URLs of news sites that it required to be blocked,[7] particularly around elections and referendums. Content filtering in Egypt has increased dramatically in the past decade,[8] and in 2018, during a referendum on a constitutional amendment, websites hosting opposition content were blocked, making 34,000 sites inaccessible.[9] Cambodia's 2018 general elections saw the government-ordered URL-blocking by Internet Service Providers of independent and international news sites, as did Zimbabwe's elections that year.[10] Content filtering in these instances typically formed part of a concerted campaign that also involved Internet shutdowns[11] and cyber-attacks on opposition sites or independent news sources. Content filtering is increasingly just one of an array of tactics used by authoritarian regimes to control the Internet.

A widening range of methods is used to filter and block Internet traffic content. The "Great Firewall of China" is believed to use the following tactics to interfere with the functioning of the Internet; IP-range blocking, DNS spoofing and redirection to inaccurate addresses, URL-filtering, DPI, malicious packet-forging to interrupt Transmission Control Protocol (TCP) transmissions, and attacks on Transport Layer Security (TLS) to essentially forge digitally signed certificates that anchor the authoritativeness of data or sources.[12] There is concern that these "Great Firewall" capabilities are being exported to a wide range of countries including Saudi Arabia, Egypt, Turkey, Thailand, Laos, Serbia, and the United Arab Emirates, which have all "agreed to cooperate with China in the digital economy to build an interconnected digital Silk Road".[13]

Collateral damage of over-blocking is increasingly widespread. In order to block specific illegal content, Turkish authorities have repeatedly used URL-blocking to cut off access to platforms including Wordpress and YouTube.[14] When DNS-blocking of Twitter.com was thwarted by some users' anti-circumvention measures, Turkey blocked the website's IP addresses,[15] again blocking a wide range of content in an untargeted measure.

---

3 https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf
4 https://english.alarabiya.net/en/media/digital/2016/12/08/Iran-bans-14-thousand-websites-and-accounts-weekly-.html
5 https://rsf.org/en/collateral-freedom?country_id=157#country_tab
6 https://www.article19.org/resources/global-expression-report-2018-19-global-freedom-of-expression-at-a-ten-year-low/
7 https://www.osce.org/representative-on-freedom-of-media/427235
8 https://thenetmonitor.org/pages/the-slippery-slope-of-internet-censorship-in-egypt
9 https://www.freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf
10 Ibid.
11 https://www.internetsociety.org/resources/doc/2019/internet-society-position-on-internet-shutdowns/
12 https://en.wikipedia.org/wiki/Great_Firewall#Active_filtering
13 https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road
14 https://policyreview.info/articles/analysis/internet-censorship-turkey
15 https://politics.slashdot.org/story/14/03/23/2145250/turkey-heightens-twitter-censorship-with-mandated-ip-blocking

Cyber security also suffers, as many of the techniques and tactics used to filter and block Internet traffic are indistinguishable from attacks, such as Man in the Middle.[16] Direct attacks and circumventions of critical parts of the Internet's global security infrastructure, including TLS, Secure Socket Layer (SSL) and the credibility of certificate-awarding structures more broadly, may also be used. Individual cyber security is also impacted when people need to use alternative approaches to access content, such as downloading software that redirects their traffic to avoid filters. These makeshift solutions subject Internet users to additional security risks.

Even in countries not immediately associated with 'digital authoritarianism', content filtering can be insidious, un-transparent and damaging. In the UK, content filtering and blocking by ISPs, based on informal government pressure rather than legislation, appears frequently to result in over-blocking. But in the absence of transparency about which content is blacklisted, or a reliable means to contest and appeal over-blocking, overall trust in content availability and accountability may be damaged.

In most countries, some people respond to content filtering by using proxies or Virtual Private Networks (VPN). While these measures can help mitigate some of the impacts of content filtering and blocking, they are beyond the capabilities of many and do not undo the harm to Internet infrastructure and to the trust and security of Internet users around the world.

If the trend towards content filtering continues, it will create a more constricted and less valuable network which prevents people around the world from enjoying many of the benefits and choices the Internet offers. At worst, and particularly with the increased availability of content filtering technologies and expertise, the Internet may fragment into a series of 'national intranets' similar to that which lies behind the 'Great Firewall of China'.

Which critical properties does content filtering affect?

Critical property 1—an accessible infrastructure with a common protocol

The only essential condition for a network or node to access the Internet is to adopt its common protocols, IP at the minimum. This "permissionless" model of the lowest possible technical barrier to entry is the basis of the Internet's rapid growth and global reach.

Government-mandated content filtering can be done by intercepting traffic entering or leaving a country, using tight control of cross-border connections by means of a national gateway or national firewall. It can also be imposed on all carriers and ISPs in a country in parallel. Both approaches breach the open and accessible infrastructure of the global Internet, and create significant, costly and complex barriers to accessing it. Content filtering and blocking in this way profoundly undermine the "permissionless" model of access to infrastructure.

The benefits this critical property should bring—global connectivity that both increases and is driven by the growing value of the Internet for everyone—are denied to Internet users and to the countries they live in. A closed and inaccessible Internet is simply not the Internet, but rather an unreliable and untrustworthy subset of it, and cannot deliver the benefits the global Internet fosters.

Critical property 3—decentralized management and a single distributed routing system

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.

Content filtering interferes with and damages the common distributed routing system the global Internet depends on, specifically by interfering with the operation of the IP numbering system and the DNS. IP-based blocking works by inserting a device into the network to block

16 https://www.internetsociety.org/resources/doc/2020/fact-sheet-man-in-the-middle-attacks/

IP addresses. DNS-blocking is done by funnelling traffic to a modified and unauthoritative DNS server that blocks certain names. Both these methods intentionally fracture the operating of the Internet's routing and addressing, with the consequence that names and addresses do not resolve consistently, authoritatively and dependably everywhere. DNS-blocking also compromises security by routing traffic to modified servers.

Requiring these methods forces infrastructure intermediaries to impose additional requirements on routing policy and DNS management that conflict with the current goals of maximizing resilience, reducing costs and optimizing traffic flows. This reduces their ability to optimize connectivity. Content filtering profoundly damages the ability of network operators to provide global reach and worldwide connectivity.

Critical property 4—common global identifiers

Every bit of data flowing between a user's computer and the applications being used is in an IP packet, and each packet has an address that says where it is going. These IP addresses allow any two systems on the Internet to find each other without ambiguity. Closely tied to IP addresses is another identifier space; the Domain Name System (DNS). The DNS has many functions, including a consistent mapping of IP addresses to domain names. The consistency of the DNS is essential to delivering predictable and secure connection for every Internet user.

Common global identifiers, particularly the IP and domain name addressing systems, deliver consistent addressing. When these systems are fractured—including by content filtering systems—networks rely on vastly sub-optimal gateways, translators and mapping tables to maintain the broken connections. Fractured namespaces create additional costs, overhead, friction and delays within the network, and reduce the security and reliability of consistent, authoritative addressing. Further, when the critical property of functioning and consistent global identifier systems is damaged, the Internet ceases to be a global network and becomes a set of imperfectly interconnected, sub-optimal networks. In the extreme cases, the mapping of these networks onto the global Internet is so fragmented and partial that the networks resemble 'national intranets', because the subset of the global Internet they provide access to is so limited.

Content filtering that uses IP-based blocking places barriers in the network, such as firewalls, that block all traffic to a set of IP addresses. A variation on IP-blocking is throttling, where a portion of traffic to an IP-number is blocked, making access slow and unreliable to discourage users. Blocking whole ranges of IP numbers 'over-blocks' wide swathes of the Internet, blocking many more than the intended sites or services. Over-blocking using the DNS causes similar 'collateral damage' when an entire website is blocked in order to cut access to specific pages or types of content on it. All these practices fragment the global identifier systems and damage the critical property that makes the Internet consistently accessible and authoritative.

Critical property 5—a technology neutral, general-purpose network

The Internet is a 'general-purpose network' because there is no defined limit to the uses its infrastructure can support. A general-purpose network requires operators of network services to perform only very basic functions: passing data packets on to its next destination without caring about their content.

Content filtering that uses DPI to intercept and examine data packets undermines this critical property by interfering with network traffic for non-operational reasons. It makes networks more complex and less efficient, with an increased need for coordination.

Conclusion

Content filtering undermines four critical properties of the Internet Way of Networking:

- **An open and accessible infrastructure with a common protocol**
- **Decentralized management and distributed routing**
- **Common global identifiers**
- **A general-purpose network**

Content filtering to address illegal content is generally inefficient, often ineffective and prone to causing unintended collateral damage to Internet users.[17] It interferes with the stability, security and resilience of the Internet and undermines four of the critical properties needed to deliver the Internet's benefits to the widest range of people.

Countries imposing content filtering impede the openness and accessibility of the global Internet by thwarting the uninterrupted flow of data to reduce access to information. The result is decreasing value and choice to the detriment of users, businesses and governments seeking to access the Internet. Content filtering undermines trust in the Internet, harms the open nature of the network and makes the Internet less resilient, less global and less valuable. Content filtering —both in its methods and its effects—undermines the basic value proposition of an open, global Internet, and denies its value and opportunities to people and to whole economies.

17 "Internet Society Perspectives on Internet Content Blocking: An Overview", 2017 https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/