The Limits of Internet Blocking: A Technical and Policy Brief on Filtering Overseas Gambling Sites

Balancing an Open Internet with the Challenges of Overseas Online Gambling

InternetNZ supports an Internet that is open, secure, and accessible for all New Zealanders. The underlying technologies that make the Internet function enable personal and economic growth, easy access to information, and innovation. However, with that comes the potential for harm from online activities including online gambling. Using technology to block and filter harmful content is appealing to policymakers because it may appear as a straightforward solution.

InternetNZ is opposed to blocking and filtering of the Internet except in very specific circumstances where the benefits of the filter outweigh the harm caused by not blocking and filtering. Our position and policy considerations regarding blocking are outlined in our 2019 paper "To Block or Not to Block".[1]

Our technical understanding of blocking and filtering leads us to conclude that blocking of overseas gambling websites, whilst technically possible, is not effective - it is becoming increasingly difficult to implement and is very easy to circumvent. For determined gamblers there are straightforward workarounds for such filters.

In addition, solving the harm caused to New Zealanders through accessing overseas gambling websites will require more than technical responses.

We recommend that you explore a suite of other solutions to the problem of New Zealanders accessing overseas gambling websites that operate outside of our legislative environment and are not regulated by the Gambling Act 2003.[2]

[1] InternetNZ September 2019 "To block or not to block" https://internetnz.nz/assets/Archives/Content_Blocking_InternetNZ.pdf

[2] Tom Pullar-Strecker 30 May 2023 "Here's how blocking New Zealanders from international gambling might work" Stuff https://www.stuff.co.nz/business/132166691/heres-how-blocking-new-zealanders-from-international-gambling-might-work

Understanding the Terminology: Geoblocking, Blocking, and Filtering

Geoblocking, blocking and filtering are terms that are broadly defined but are technically quite different from each other. Below are the definitions generally used in the global Internet community.

- ***Filtering*** involves scanning Internet traffic using a list of predetermined blocked URLs, domain names, or keywords. When the filter detects an attempt to access a blocked page it may redirect the user to a different website to display a "page not found" or "unavailable for legal reasons" message. Filtering is typically implemented at the organisational or Internet Service Provider (ISP) level. An example of filtering is the child sexual abuse material filter operated by the Department of Internal Affairs.[3]
- ***Blocking*** is the practice of restricting access to a particular website or content for a group of users. Generally, it is mandated at the organisation or government level. Usually, it redirects a person attempting to access the site to a 'stop' page or some other form of a 'page not found' message.
- ***Geoblocking*** is the practice of restricting access to a website or content based on the location of the person seeking to access the content. For example, BBC iPlayer will not allow full access to its content to someone in New Zealand due to licensing arrangements. Geoblocking is usually done at the website end rather than the customer end. Often the organisations that use geoblocking as a solution have a copyright-related reason to do so. A further example of geoblocking is Digital Boost, which was geoblocked outside New Zealand because it was a taxpayer-funded programme and they wanted to restrict services to New Zealand small and medium enterprises.

All types of content blocking involve an element of surveillance of a person's Internet activity and may have privacy impacts. An extreme example of such surveillance is known as the Great Firewall of China. China has a very sophisticated blocking and filtering system that prevents its citizens from accessing a range of websites and media. This is possible due to its high level of control over access to the Internet in China.

Internationally there are three key forms of approach used by governments in terms of Internet Management[4]. These can be summarised as :

- State control and protection in countries like China or Viet Nam
- Personal privacy priority as in European legislation[5]
- Business freedom and priority for innovation as is supported in countries like the United States of America.

[3] Department of Internal Affairs, 'Censorship DCEFS Public Information Pack', https://www.dia.govt.nz/Censorship-DCEFS-Public-Information-Pack#3

[4] Mauro Santaniello, 2021, "From governance denial to State Regulation: a controversy-based typology of internet governance models" https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003008309-3/governance-denial-state-regulation-mauro-santaniello

[5] Internet Policy Review, 2021, "Extraterritorial Application of the GDPR: promoting European values or power?' https://policyreview.info/articles/analysis/extraterritorial-application-gdpr-promoting-european-values-or-power and Number Resource Society "Impact of Internet Governance on Digital Privacy"

Each takes a different approach to blocking, filtering, and encryption.

Increasingly, like-minded overseas jurisdictions are using partnerships with the banking sector to limit phishing, scamming and fraud activities by targeting money transfers and changes in customers' spending behaviours. These activities are generally coupled with support and education that enables people to develop their own defences. The New Zealand banking sector has noted that this approach will not be effective for online gambling.[6]

Technical Feasibility and Obstacles to Blocking

Blocking and filtering can be implemented at the infrastructure level where core Internet protocols make connections and deliver information. For the purposes of this advice, infrastructure includes Internet Service Providers (ISPs), the Internet Protocol (IP), the Domain Name System (DNS), Content Delivery Networks (CDNs) and servers that host copies of content.[7]

People connecting to the Internet do so through an ISP. ISPs have the technical ability to modify connections to domain names, unencrypted URLs, and IP addresses, but doing so goes against the end-to-end principle which requires that connections are controlled by the people using them.[8] It is practically impossible to do this for URLs in an encrypted HTTPS environment which is used by most Internet users.[9]

In some parts of the world, governments implement a block through more direct control of Internet connections.[10] In a democratic country like New Zealand, Internet services are provided by independent market players, meaning cooperation from commercial and independent ISPs would be needed to implement any of the blocking methods set out in the following table.

[6] Tom Pullar-Strecker 30 May 2023 "Here's how blocking New Zealanders from international gambling might work" Stuff https://www.stuff.co.nz/business/132166691/heres-how-blocking-new-zealanders-from-international-gambling-might-work

[7] For a detailed look at how the Internet works, see InternetNZ's Internet Openness: what it is and why it matters (2019). See also ISOC 'Content Blocking Overview (2017), https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

[8] Jerome H Saltzer, DP Reed and David D Clark "End-to-end Arguments in System Design" (1984) 2 ACM Trans Comput Syst 277

[9] Over 90% by 2021 - Electronic Frontier Foundation HTTPS Everywhere https://www.eff.org/https-everywhere

[10] Can include a range of methods including inspecting all data packets sent through international transfer points, requiring enforcement at the ISP level or other techniques.

[11]	DNS filter	IP filter	URL filter	Deep packet inspection
Overview	An ISP might configure their servers to block or redirect lookups for certain domain names.	A network filter can block specific IP addresses from successfully returning a response or route traffic via a particular path.	A URL filter can block specific pages within a website but is limited to unencrypted traffic. In 2024 over 95% of pages were accessed via encrypted HTTPS, according to Google Chrome statistics, severely reducing the effectiveness of this method.[12]	Blocking based on deep packet inspection is where individual packets of data are inspected to identify whether they contain keywords or components of images, and flagged web pages or elements are blocked from the end user. Not particularly effective on encrypted traffic.
Limitations of this method	Users can easily circumvent this method by configuring their routers to use an alternative DNS service.	IP addresses are easy to change, so can be easily evaded by the content publisher. IP block lists are often long and hard to maintain due to the ease of evasion.	Encryption or use of a VPN renders this technique ineffective.	Encryption or use of a VPN renders this technique ineffective. Mass surveillance of end users is required.
Risks of using this method	Blocks access to all content served by a domain name, potentially blocking access to non-harmful, legal information.	An IP filter blocks all content from one IP address, blocking legal, non-harmful content as well as illegal content from that address.	URL filtering can cause performance problems, decreasing overall speed and reliability.	This kind of 'content aware' filtering can cause performance issues for the network as it requires all packets to be passed through inspection engines, introducing network delays for legitimate content.
	Undermines the integrity and chain of trust behind the DNS system.	A single IP address can serve many websites (often when a website is hosted on a CMS like Squarespace or Wix) so this method is a blunt tool that can cause collateral damage. An example could be Viet Nam's blocking of Facebook in response to online criticism.		False positives are common, as keywords may be acceptable in one context and not in another. An example could be a pornography-related block causing medical students to not be able to look up certain medical words.

[11] This table does not cover 'geoblocking' under the definition listed above (the practice of restricting access to a website or content based on the location of the person seeking to access the content) and instead covers how you might block or filter. This is because geoblocking is usually implemented at the website end rather than at a system or national level.

[12] Google Transparency Report "HTTPS encryption on the web" https://transparencyreport.google.com/https/overview?hl=en

Any instances where this blocking method is justifiable?	ISPs may use DNS filters to protect against security threats such as malware or known phishing domains. These filters are commonplace and non-controversial	These are the methods used by NZ’s Digital Child Exploitation Filtering System[13]	

Blocking through infrastructure contributes to Internet Fragmentation[14] whereby the open Internet starts breaking into smaller, disconnected parts, resulting in people in different countries having very different online experiences for technical, commercial, or political reasons. Blocking overseas online gambling websites could be viewed as a form of Internet fragmentation.[15] Internationally, Internet Fragmentation is seen to undermine the open international nature of the Internet, which can undermine the benefits of the Internet, including social and economic connection.[16]

Global Internet Fragmentation: Risks and Realities

InternetNZ is generally opposed to blocking and filtering of the Internet. It is technically very difficult and easy to circumvent.

Since InternetNZ submitted on proposed online gambling regulations in 2019, and wrote “To Block or Not to Block”[17], encryption technology and other cybersecurity technologies that protect people’s privacy online have become increasingly common. Often these settings are the default for browsers or are easily implemented by an Internet user.

Blocking is hard to target as technical blocks are blunt tools which can impact non-targeted content. This may be through blocking entire domain names or IP addresses which also deliver non-harmful content, or blocking false positives, where non-harmful content is read as harmful by an algorithm or filter. Blocking and filtering can create security risks as methods that reroute traffic can open the system up to abuse by attackers. URL filters only work on unencrypted traffic. Filtering IP addresses would be very difficult as there are not enough IP addresses to go around and online content often shares an IP address.

[13] Department of Internal Affairs, ‘Censorship DCEFS Public Information Pack’, https://www.dia.govt.nz/Censorship-DCEFS-Public-Information-Pack#3.

[14] Vivien Maidaborn, 2024, “Examining Internet Fragmentatoin at ICANN 79” https://internetnz.nz/news-and-articles/examining-internet-fragmentation-at-icann79/

[15] Andrew Sullivan 10 July 2023 “A Fragmented Internet is a Threat to the Future of Global Business” Forbes https://www.forbes.com/councils/forbestechcouncil/2023/07/10/a-fragmented-internet-is-a-threat-to-the-future-of-global-business/ or Internet Society “Internet Fragmentation: An Explainer” https://www.internetsociety.org/resources/internet-fragmentation/

[16] Nick Merrill and Konstantinos Komaitis 17 December 2020 “The consequences of a fragmenting, less global internet” The Brookings Institute https://www.brookings.edu/articles/the-consequences-of-a-fragmenting-less-global-internet/

[17] InternetNZ September 2019 “To block or not to block” https://internetnz.nz/assets/Archives/Content_Blocking_InternetNZ.pdf

Controlling online gambling websites and their use by New Zealanders will not be a simple task. The Department of Internal Affairs encourages New Zealand ISPs to operate the child exploitation and sexual abuse material filter, which has high uptake so is largely effective. This filter has a high level of general acceptance due to the highly unacceptable nature of the content. Online gambling poses different harms and would require a different cost-benefit analysis. Although applying another filter here might seem logical, the growing use of privacy and security protocols like TLS 1.3 ECH, DNS over HTTPS, and DNS over TLS[18] makes it unlikely that such a filter would effectively protect those most vulnerable to online gambling harm. Given technology trends, we expect this effectiveness to diminish even further.

The above technological trends enable the user to prevent unauthorised users from viewing their online activity.

Our browsers are set up to protect us from bad actors online and to protect our privacy by default. Additionally, while a filter applies to both apps and browsers, the use of apps introduces new levels of evasive and secretive tactics, making the use of such a filter complicated.

Conclusion: Why Blocking and Filtering May Not Be the Answer

Blocking of overseas gambling websites will not solve the issue of New Zealanders using these websites. Due to how devices and apps are set up, blocking or filtering of overseas gambling websites is easily circumvented by those determined to gamble in this way.

The processes users would employ to circumnavigate a block might include the use of a Virtual Private Network (VPN) which works by rerouting Internet traffic so that it appears to be coming from a different place to its original location, or encryption technology which works by scrambling data so that only authorised participants at each end can see what’s in data packets being sent.

We recommend seeking other solutions

We recommend that the government not use a block or filter for overseas gambling websites. Instead, we suggest exploring alternative solutions that ensure compliance with New Zealand's Gambling Act 2003 and its regulations, which aim to control gambling growth and minimise harm, among other objectives.

While implementing compliance measures for overseas gambling sites may be technically challenging and easily circumvented, there are other policy options worth considering. It is important to recognise that enforcing compliance may be

[18] TLS 1.3 ECH - Transport Layer Security 1.3 Encrypted Client Hello - a system that prevents and ISP or government from being able to determine which website is being visited
DNS over HTTPS - Domain Name System over Hypertext Transfer Protocol Secure - a system that encrypts DNS traffic only between the end-user and the server they use to resolve domain names into IP addresses
DNS over TLS - Domain Name System over Transport Layer Security - a system that encrypts DNS traffic only between the end-user and the server they use to resolve domain names into IP addresses

difficult given that many of these websites operate from outside New Zealand's jurisdiction.[19]

We encourage you and your officials to continue work on this matter. We welcome further dialogue on how best to reduce overseas online gambling in New Zealand.

[19] Tom Pullar-Strecker 30 May 2023 “Here’s how blocking New Zealanders from international gambling might work” Stuff https://www.stuff.co.nz/business/132166691/heres-how-blocking-new-zealanders-from-international-gambling-might-work