Version 23 May 2016

Why DNS blocking has no place in Dutch law

This viewpoint has been written by Maarten Simon and Marco Davids, both of whom work for SIDN, the registry for the .nl domain. Simon and Davids' viewpoint is shared by Digital Infrastructure Netherlands (DINL), a foundation through which SIDN cooperates with AMS-IX, the Dutch Datacenter Association, DHPA, ISPConnect, Netherlands ICT, NlNet, SURFnet and the Registrars' Association.

In brief

The beauty of the internet is that it connects people all over the world. Interfering with the internet's success formula by modifying its technical infrastructure threatens the basic fabric of the system. Furthermore, blocking domain names entails risk and is unlikely to be effective. The provisions of the Gaming Bill that would give the Netherlands Gaming Authority (KSA) the power to order the blocking of websites should therefore be removed.

What

In the Netherlands, a Gaming Bill has been brought before parliament. Section 34n of the bill would give the KSA the power to indirectly require ISPs (e.g. KPN, Ziggo, etc) to block domain names linked to gambling websites that are illegal in the Netherlands. The aim being to prevent Dutch users accessing the websites in question (or, at least, to make accessing them more difficult).

Why

The KSA's new power has been proposed with the intention of curbing the activities of on-line gambling providers that are not legal in the Netherlands. That in turn is intended to protect users against addiction and fraud; legal providers against unfair competition, and the state against loss of tax revenue.

Why it's not a good idea

a. The principle

The internet's strength is that it is a global system, which works in the same way for everyone, everywhere. That is achieved by everyone conforming to a common set of protocols, which underpin the internet's infrastructure. Users assume that the internet works in accordance with the protocols, even if they rarely or never give those protocols any conscious consideration.

Requiring ISPs to block domain names (DNS blocking) constitutes interference with one of the internet's primary protocols: the Domain Name System (DNS). It therefore compromises the working of the internet.[1] That in turns threatens the neutrality and functional reliability of the internet as a technical system. If a precedent is set and the scale of interference increases, the performance of the internet (and therefore confidence in it) will be undermined. That will lead to the development and use of other methods of communication that do not rely on the DNS. A risk of fragmentation will consequently arise and one of the primary reasons for the internet's success – its uniform global character – will be removed.

There is increasing recognition of such dangers, as illustrated by the foundering of the multinational Anti-Counterfeiting Trade Agreement (ACTA) and the SOPA and PIPA bills in the US. Both those bills proposed the use of

[1] Such interference will be increasingly visible to users due to the growing use of DNSSEC, an extension to the DNS designed to ensure that traffic is not intercepted.

DNS blocking as a means of protecting intellectual property rights. Their rejection was due in part to intensive lobbying by the international internet community, based upon the principles outlined above.[2]

Furthermore, the Netherlands Scientific Council for Government Policy (WRR) explicitly highlighted the dangers in its report *The public core of the Internet*, published last spring.[3] That report's main conclusion is that 'governments need to exercise enormous restraint when considering policies, legislation and operational activities that intervene in the Internet's core protocols' (p 85). The report also stays (p 84) that, 'Ideally, the international norm should be non-intervention in the core protocols and basic technology of the public Internet.'

The report goes on to advise the government to adopt a diplomatic approach that gives precedence to the internet's public core. The WRR also correctly emphasises the importance of the Netherlands at least practising what it preaches. The Netherlands cannot campaign internationally for protection of the internet's public core, while at home eroding that public core by blocking gambling sites that are illegal within its own borders.

b. The dangers

DNS blocking by ISPs is not without dangers for third parties. Anyone can make a typing error, e.g. putting '.nl' after a domain name out of habit, when it should have been '.com'. An error in a DNS block could result in the wrong domain name being made unreachable.[4]

Another potential problem is 'over-blocking': if a gambling site uses a subdomain name (gambling.provider.com), the whole of the parent domain (provider.com) could be taken off line.

What's more, action from both the KSA and the ISPs would be needed to keep the list of blocked domain names up to date. Experience in Belgium suggests that such arrangements can't always be relied upon. One of the domain names on the blacklist of Belgium's gaming authority is already freely available for re-registration. Any new registrant may be surprised to discover that their domain can't be reached from Belgium.

c. Lack of effectiveness

Requiring an ISP to block a domain name merely prevents that ISP's clients from reaching the relevant website via the ISP's system. The domain name remains active for the rest of the world, and everyone else can still visit the website.

Consequently, even the ISP's clients can reach the website if they use alternative routes. Some of the ISP's clients are liable to actively seek out a way of circumventing the block,[5] while others may be helped to reach the site by the illegal gambling provider or a third party, without the clients in question having to take the initiative.[6]

---

[2] A clear summary of the arguments against DNS Blocking is given by the Internet Society in http://www.internetsociety.org/sites/default/files/pdf/dns-filtering_20110915.pdf

[3] http://www.wrr.nl/publicaties/publicatie/article/de-publieke-kern-van-het-internet-1/

[4] An example of how things went wrong in Denmark: https://edri.org/edrigramnumber10-5danish-filter-blocks-google-facebook/

[5] A few moments with a search engine is all it takes to identify options such as public DNS servers, VPN services and TOR.

[6] A website whose domain name is blocked can be reached using its IP address or using a clickable link in an advert, which doesn't rely on the DNS. The website can also be approached indirectly via other (as yet) unblocked domain names.

When the case of Ziggo and XS4ALL versus Brein went to the Court of Appeal, a report by TNO was presented in evidence. In line with other experts, TNO concluded that the effect of blocking domain names (in that case thepiratebay.se) was very limited. The ease with which DNS blocks can be circumvented by almost any internet user with the inclination was illustrated by the large-scale use of workarounds during the period that thepiratebay.se was blocked.

The effect of the KSA's proposed blocking powers will be further restricted by the fact that the authority can act only against domain names linked to websites 'aimed specifically at the Netherlands'. Many of the sites that are illegal in the Netherlands are entirely legitimate in other countries. For that reason, the KSA already rightly limits itself to tackling providers that specifically target the Dutch market.[7] Meanwhile, there is absolutely nothing to prevent Dutch people using any of the very many non-Dutch gambling sites that target wider markets.

Conclusion

Blocking domain names will probably have very little effect on the intended targets. It will, however, introduce the risk of errors, with potentially significant adverse implications for innocent parties. More fundamentally, it will ultimately threaten the unity of the internet – something that the WRR has urged the Netherlands to work to protect.

Alternatives

Although the expertise of SIDN and DINL lies primarily in other fields, we would be pleased to contribute our ideas to any effort to identify alternative and effective means of preventing illegal gambling in the Netherlands.

We feel that the most obvious solution is to facilitate ready access to an ample number of competitive and attractive legal gambling providers. It is our belief that most Dutch people would opt for a good legal provider in preference to an illegal provider, because of the convenience and/or the perceived trustworthiness of the legal provider. Many gamblers are reluctant to use illegal sites, because they fear the games may be rigged and that they may not get paid if they win.

Furthermore, as with all internet-related issues, the Netherlands and other nations must do more to promote international collaboration. It is an inescapable fact that the internet is a global institution. Hence, collaboration is always necessary to realise any effective change.

Finally, we feel that the scope for using payment transaction blocks to achieve the aims of the bill's domain name blocks warrants examination. We do not, however, presume to have the expertise to comment on the feasibility or desirability of such a strategy ourselves.

For more information, please contact:

Maarten Simon
maarten.simon@sidn.nl

or

Marco Davids
marco.davids@sidn.nl

[7] http://www.kansspelautoriteit.nl/onderwerpen-0/kansspelen-internet/aanpak-online/