The Response of European Digital Rights to:

Green Paper on on-line gambling in the Internal Market

SEC (2011) 321 final

JULY 2011

Table of Contents

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
E-Mail: brussels@edri.org, http://www.edri.org

Introduction

European Digital Rights (EDRi) is an association of 28 privacy and digital civil rights associations from 18 European countries. We have a particular interest in open and balanced approaches to access to internet services and welcome the opportunity to respond to the European Commission's Green Paper. Due to our focus, we will respond only to the set of questions in the Green Paper that focus on the measures used for restriction of "unauthorised" and cross-border on-line gambling services.

We strongly support the public policy goals of the European Commission in this dossier – namely to protect consumers, to combat fraud and to fight money laundering.

However, we regret that much of this debate has been driven by Member States' eagerness to protect tax revenues from domestic services and revenues from national gambling monopolies. This approach is contrary to the basic principles of the European Union and any online restrictions undertaken for this purpose are unquestionably disproportionate, unnecessary and unequivocally contrary to the European Convention on Human Rights.

It is nothing less than an affront shared European values to see the Belgian state, for example, willfully failing to protect consumers from allegedly fraudulent[1] TV gameshows and, at the same time, deciding to block access to gambling sites that are legally operating elsewhere in the European Union.[2] This is not consumer protection, it is naked protectionism. Direct or inadvertent support by the European Commission for such policies must be avoided.

Questions:

(50) Are any of the methods mentioned above, or any other technical means, applied at national level to limit access to on-line gambling services or to restrict payment services? Are you aware of any cross-border initiative(s) aimed at enforcing such methods? How do you assess their effectiveness in the field of online gambling?

(51) What are your views on the relative merits of the methods mentioned above as well as any other technical means to limit access to gambling services or payment services?

The consultation document refers to “IP blocking”. It is not obvious to us whether this is IP address blocking (where an access provider limits access to specific IP addresses) or location-based blocking (by online services which block visitors based on the IP address of their internet connection). The latter technology presents no fundamental rights issues, is not intrusive and its (in)effectiveness is broadly identical to DNS blocking, which can be easily circumvented (see the “effectiveness” section below).

1 http://www.een.be/programmas/basta/de-mol-in-het-belspel
2 Wet van 7 Mei 1999 op de kansspelen, de weddenschappen, de kansspelinrichtingen en de bescherming van de spelers.

From this point forward in this document “IP blocking” will be understood as the former technology, namely, blocking of access *to* specific IP addresses by Internet access providers.

With regard to these two questions, EDRI’s opinion is that the use of Internet Protocol (IP) “blocking” and Domain Name System (DNS) “blocking” infringes human rights and raises very serious security and technical concerns. Below, we will provide the reasons that lead us to this conclusion. For the sake of convenience, our response would be separated on three parts, namely, (1) Effectiveness of IP Blocking and DNS-based blocking, (2) Legality of the IP Blocking and DNS-based blocking, (3) Legality of the IP Blocking and DNS-based blocking through non-legislative measures.

Effectiveness of IP Blocking and DNS-based blocking

IP address and DNS blocking are not effective measures for preventing access to digital content in general because they can be easily circumvented. In fact, the use of the word “blocking” is fundamentally incorrect as, due to the resilience of the Internet, the technologies described in the Commission’s paper can only restrict (with varying and limited degrees of effectiveness) but not “block” the online resources that are targeted. To remain consistent with the terminology used in the Commission's consultation document, we will use the term “blocking”, by which we mean “access restriction”. Below, we explain how easy is to circumvent the IP Blocking and DNS-based blocking.

First, there are online proxy websites, where a user can simply input the URL (for example www.blockedexample.com) of the “blocked” page and they will receive immediate access. Second, people who access the Internet using privacy enhancing technologies (the development and use of which are actively encouraged by the European Commission) are likely to find themselves accidentally circumventing blocking systems. Thirdly, there are numerous instructional videos online which explain in five minutes or less how to bypass your Internet provider’s equipment and therefore any blocking that it has installed. People using services like anonymizer.com or openvpn.com in order to, for example, watch TV shows in other countries that are restricted to users that have domestic IP addresses will circumvent the blocking system without even realising that they are doing so. This raises two distinct problems:

- insofar as the blocking system would ostensibly protect citizens from fraudulent websites, they could reasonably assume that any website that is accessible to them is authorised by the state, thereby creating a false sense of security;
- the restriction limits the freedoms detailed in the Charter of Fundamental Rights and such restrictions are only permissible if they “are necessary and genuinely meet objectives of general interest” (article 52), which technically limited approaches clearly fail to do.

In its communication, the Commission explains in a footnote that “millions of re-directions” allegedly happen every week as a result of blocking in Italy (thereby, we assume, seeking to demonstrate “effectiveness”. In an adult population of approximately forty million (and assuming “millions of redirections” means at least two million), this equates to a minimum of approximately 5% of the adult population hitting the blocking system every week or 2.6 hits per adult per year!

This statistic is therefore clearly quite obviously implausible and could be explained by a mixture of two factors. Firstly, a consistent figure of millions of redirections *every* week could be explained by the it being so easy to access foreign gambling websites that, week after week, millions of Italians are not discouraged by hitting a blocking system, because they know that they will find another route to a foreign site easily. Alternatively and/or additionally, a huge amount of online traffic is generated by search engine “spiders” searching for new information. The EDRi.org website, for example, had significantly in excess of 100,000 such “hits” in May, 2011. If it had been blocked, then there would have been statistics of this number of redirects which, in reality, had no human involvement at all.

Another reason why there would be a high level of search engine traffic on the Italian blocking page is because it is widely referenced on the web – according to Google, there are 1650 sites linking to the blocking page (http://217.175.53.72/index.html). This will drive large amounts of search engine traffic to this page and many people will click on the link to see what the blocking page looks like, increasing the traffic still further.

More invasive and effective technologies do exist, such as “deep packet inspection” (DPI) which, if deployed on an internet access provider's network can open each packet of data to establish where it is coming from, where it is going to and the nature of the file in question. Insofar as a site has already been identified as being illegal/unauthorised and as long as the IP address has not changed since being added to the system, this technology would be comparatively effective. However, this amounts to a major interference with the right to privacy protected by Article 8 of the European Convention on Human Rights. Furthermore, being expensive, the obligatory implementation of DPI would have major negative consequences for the functioning of the access provider market. This negative impact would be re-enforced if the DPI were then to be re-used for anti-competitive practices, such as blocking of legal services that were in competition with the access providers' services.[3]

Legality of the IP Blocking and DNS-based blocking

IP address blocking has a vast capacity for accidentally blocking unrelated websites. According to a 2003 study by Harvard University,[4] most websites

3 Existing practice in the mobile market, in partiuclar, shows that this is a real risk. See, for example http://moconews.net/article/419-german-carrier-t-mobile-blocking-skype/

4 http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/

share IP addresses, with unique IP addresses sometimes being used for hundreds of individual and otherwise unrelated websites. Blocking an IP address therefore involves, almost inevitably, blocking large numbers of innocent websites.

DNS-based blocking can also restrict the access to domain names that do not link to websites offering online gambling services. However, this type of blocking can be done in a more targeted way than IP address blocking, but also suffers from severe technical limitations, particularly because it is very easy to circumvent – even accidentally. Indeed, the European Commission itself will accidentally circumvent the planned blocking of gambling sites in Belgium because the computer equipment (DNS servers) it uses to access the Internet are based in Luxembourg.

Any move towards effective blocking mechanisms will ultimately lead to deep packet inspection. Which, as stated, is the most invasive, effective and counter-productive method of blocking access to specific content. It is exceptionally privacy intrusive and would entail significant collateral damage for the free speech, competition and the functioning of the access provider and online services market in Europe.

With regard to the blocking of legal online gambling sites, there are two possible reasons:

- To protect citizens from fraud and/or money laundering. This would only be legal if the size of the problem were such that it would render blocking "necessary in a democratic society," if it were effective *and* if less restrictive options, such as efficient cooperation with payment service providers or the use of trustmark schemes proved ineffective.

In order to use any online gambling service, some form of electronic payment service must be used. European financial institutions are subject *inter alia* to Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. To date, no evidence has been produced to suggest that this Directive is failing to function effectively and, if it is functioning ineffectively, that it cannot be improved in a way which would obviate concerns regarding the use of online gambling services for money laundering purposes.

- As a general consumer protection measure, such as to protect citizens from gambling addiction. Here again, it would only be legal if it the size of the problem makes such a policy necessary in a democratic society, if blocking would effectively address the problem and if less restrictive alternatives did not exist. There is absolutely no evidence that this is the case. It would certainly be worthwhile for the Commission – or a Member State that is using addiction as a justification for blocking – to tender for a study to ascertain the size of the online gambling problem, assess the key differences between the nature of the problem online and offline and produce a full range of possible measures that

could be taken. Only at that stage could the issues of proportionality and less restrictive alternatives be adequately addressed.

Neither of these points has been addressed adequately, including by Member States that have already introduced blocking. Consequently this basis for the introduction of blocking is also not a valid legal reason. In this interest of harmonising the single market, such as it is in this context, we would urge the Commission to request the removal of web blocking systems that currently exist in Europe, even if imposing this as a legal obligation is legally problematic at the moment.

It is our understanding that the Belgian authorities intend to investigate users that are redirected by the Belgian blocking system, due to be implemented in January 2011. This not alone turns the blocking system into a permanent surveillance system and a gross breach of privacy, it also runs counter to the normal police view that people tend to hit blocking systems accidentally – as illustrated by an Irish police letter to Irish ISPs which explained that "it is clear that genuine ISP customers are inadvertently accessing such material".[5] (referring to people hitting the blocking system for child abuse material).

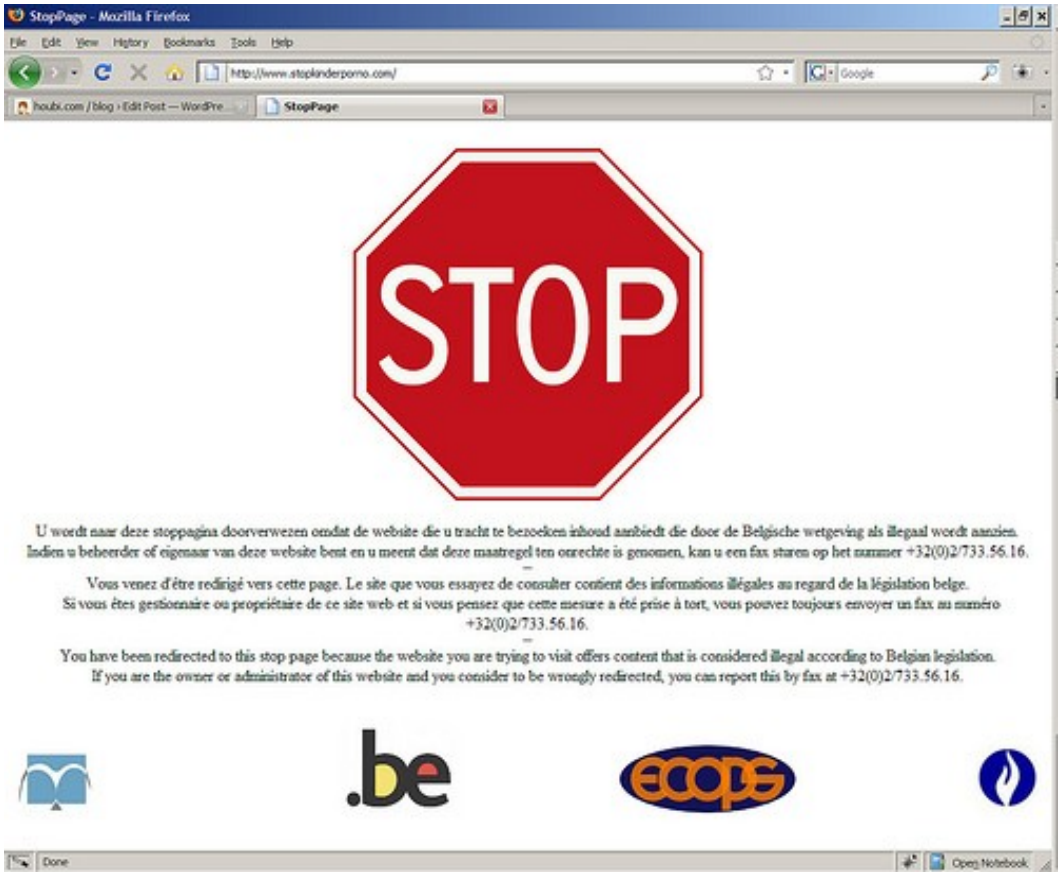

Fig 1: Example of an existing EU blocking page (the page in the example was used to block an anti-child abuse website). The English text says "you have been redirected to this stop page because the website you are trying to visit offers content that is considered illegal under Belgian legislation. If you are the owner or administrator of this

5 http://www.scribd.com/doc/51018185/Garda-Letter-to-ISPs-Requesting-Blocking

website and you consider to be wrongly redirected, you can report this by fax to +32(0)2/733.56.16."

In short, the IP blocking and DNS-based blocking and, most particularly, deep packet inspection of online gambling websites is unquestionably contrary to Articles 8 (privacy) and 10 (freedom of communication) of the European Convention on Human Rights and Article 52 of Charter of Fundamental Rights.

We would also point out in this context that a member of the current College of Commissioners has given a strong undertaking to oppose blocking in any context outside child exploitation. In May of 2010, Commissioner Malmström[6] unequivocally stated that "the Commission has absolutely no plans to propose blocking of other types of content - *and I would personally very strongly oppose any such idea"*.

The illegality of blocking can also be also be adduced from Advocate General Cruz Villalón's Opinion[7] in Case C-070/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam). In this case, Mr Villalón stated that a measure ordering an internet service provider to install a system for filtering and blocking electronic communications in order to protect intellectual property rights in principle infringes fundamental rights. According to Advocate General, in order to be permissible, such a measure must comply with the conditions laid down in the Charter of Fundamental Rights to govern restrictions on the exercise of rights. With regard to the conditions that need to be met for such a measure to be legal, in paragraph 113 of its opinion, the Advocate General states that the charter requires that all limitations of the enjoyment of the rights and freedoms that it recognizes respect the principle of proportionality, respond to the principle of necessity and effectively seek to fulfill objectives of general interest recognised by the Union or that respond to the need to protect the rights and liberties of others.

Mission creep, function creep and technology creep

To assess proportionality, attention also needs to be given to the political, judicial and practical effects of the introduction of blocking, particularly in Member States where blocking is not in force. In Italy, blocking was introduced for a narrow range of issues, but this grew to a situation where it is used for an ever-growing range of content (4771 sites are currently blocked). It is now undermining the rule of law and free speech as a system has recently been introduced to block sites in the absence of a court order. Completely legal virtual private network services are now also being blocked (due to fears of deliberate or accidental "misuse" to circumvent blocking) and, most recently, criminal charges have been brought against Internet access providers for failing to "effectively" block a site accused of facilitating intellectual property

6 http://www.meldpunt-kinderporno.nl/files/Biblio/Speech-Malmstrom-Combating-sexual-abuse06_05_2010.pdf
7 http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10

infringements. Long term experience in all EU countries except (for the moment) Sweden that have introduced blocking is that it always has unpredictable side-effects. This must also be taken into account in any proportionality assessment.

The inevitable damage caused by mission creep will be particularly felt in countries that have not yet imposed blocking for any purpose.

Legality of the IP Blocking and DNS-based blocking through non-legislative measures

Discussions on Internet regulation in general, at nation state, regional and global level are increasingly leaning towards “self-regulatory” measures rather than them having a legal basis, as shown by the Italian example above. However, IP blocking and DNS-based blocking through non-legislative measures is contrary to the Article 10(2) from the European Convention on Human Rights, which require that the restriction of the right of expression may be subject to such formalities, conditions, restrictions or penalties as are “prescribed by law”.

The illegality of the blocking through non-legislative measures was confirmed by the Commission in the impact assessment it prepared to accompany the proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework decision 2004/68/JHA.[8] In the particular text, the Commission assessed the extra-judicial blocking as follows: "More problematic may be the compliance with the requirement that the interference in this fundamental right must be "prescribed by law", which implies that a valid legal basis in domestic law must exist" (page 30). Then, the Commission concluded that "such measures must indeed be subject to law, or they are illegal" (page 37).

Finally, EDRi would draw attention to the report[9] of UN Special Rapporteur on Freedom of Expression with regard to the dangers, abuses and illegality of this approach. More recently, a report from the OSCE reached broadly the same conclusions.[10]

Conclusion

European Digital Rights believes that:

- Blocking of websites that are legally operating in other EU countries in order to protect tax revenues or local gambling monopolies is grossly disproportionate;

8 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0355:FIN:EN:PDF

9 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

10 http://www.osce.org/fom/80735

- Blocking of possibly illegal foreign websites is not the least restrictive available alternative and other approaches have not been adequately tested;
- IP address and DNS blocking are technically limited and create the risk both of innocent websites being blocked and being accidentally circumvented, giving end-users the false belief that the website they are visiting is approved. The ease of deliberate circumvention is such as to render the measure ineffective and therefore contrary to both the EU Charter and European Convention on Human Rights. Deep packet inspection is disproportionate and breaches both article 8 and 10 of the European Convention on Human Rights;
- Blocking through non-legislative measures (whether “voluntary” or imposed by non-judicial authorities) is contrary to the Article 10(2) from the European Convention on Human Rights, which require that the restriction of the right of expression may be subject to such formalities, conditions, restrictions or penalties as are “prescribed by law” and Article 52 of the Charter of Fundamental Rights;
- Restrictions must not be imposed “by proxy” using intermediaries coerced into action by a intermediary content liability regime.