July 2011

Position of the Net Users' Rights Protection Association (NURPA)

on

The Green Paper on on-line gambling in the Internal Market
(COM(2011) 128 final)

Net Users' Rights Protection Association
Identification number in the register: 80339855034-02

Introduction

The Net Users' Rights Protection Association (NURPA) highly appreciates the opportunity to comment on the European Commission's Green paper on online gambling in the Internal Market COM(2011) 128 final (the ‘Green paper’).

The NURPA is a Belgian advocacy group which promotes and protects digital rights and the founding principles of the Internet. Since technologies increasingly influence our lives as citizens, consumers, artists and professionals, the NURPA defends fundamental rights and freedoms in the networked world wherever they might come under attack. As a non-profit organization, the NURPA is dedicated to the protection of privacy, digital rights and civil liberties.

This submission does not address all the points raised in the Commission’s Green Paper. Rather, it is limited to the issues of payment blocking and liability regimes for Internet Service Providers (section 2.4).

In short, the NURPA concludes as follows:

- The methods proposed by the Commission in section 2.4 of the Green paper to limit access to gambling services on the Internet are not effective;
- The proposed measures are disproportionate and unnecessary and therefore violate fundamental rights;
- The proposed measures carry unintended consequences;
- The proposed measures are therefore not appropriate for a regulation in the field of online gambling.

The NURPA supports the Commission's goal to address the problems of gambling addiction and fraud, to oppose the development of black markets and to regulate in the field of 'grey' markets. In principle, the NURPA welcomes the approach of the proposal and presents its comments on the individual questions as follows:

> *(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 on-line gambling?*

1. Methods applied at national level to limit access to on-line gambling services

The French government introduced the law 2010-476 in order to block non-homologated gambling sites [1]. This led to the creation of the French online gambling regulation authority Autorité de Régulation des Jeux En Ligne (ARJEL).

On 7 July 2010, the ARJEL requested the blocking of the gambling service StanJames. As a result, on 6 August 2010, the Tribunal de Grande Instance ordered French ISPs to block websites 'by all means' [2]: « blocage du nom de domaine, de l'adresse IP connue, de l'URL, ou par analyse du contenu des messages. » As a result the online gambling website StanJames has been blocked by French ISPs. Almost immediately, a mirror website called Arjel-Stanjames.com was created which redirected French Internet users to the original website StanJames.

In the beginning of 2011, the French regulation authority requested to block another gambling service, 5Dimes. However, seven ISPs (Orange, SFR, Numericable, Free, Bouygues Telecom, Darty Telecom and Auchan Telecom) opposed the request during a hearing at the High Court of Paris. The ISPs considered that web blocking measures are inefficient and would create a dangerous precedent by blocking without a judge's decision [3].

2. Effectiveness of methods

Despite the lack of an exact definition of 'IP blocking', the NURPA considers that this term is used in the Green paper in order to indicate that a provider restricts the access to a specific IP address.

Furthermore, a first leak of the Commission's Green paper stated itself that blocking is 'technically challenging and costly' and that it will still leave a 'significant' number of illegal sites available [4].

At a European level, there are many examples of blocking or filtering attempts that were not effective (the following list is not exhaustive):

1. http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022204510&fastPos=1&fastReqId=232372637&categorieLien=cid&oldAction=rechTexte
2. http://www.scribd.com/doc/35479988/Ordonnance06082010
3. http://www.latribune.fr/technos-medias/medias/20110317trib000608945/les-operateurs-telecoms-arc-boutes-contre-le-filtrage-des-sites-de-paris-sportifs-illegaux.html
4. http://www.statewatch.org/news/2011/jan/eu-com-draft-green-paper-on-internet-gambling.pdf

- Belgium: Despite the fact that the website ‘Stopkinderporno’ was blocked in 2009, it remains easily accessible using any circumvention means described below;
- Italy: DNS-filtering was very rapidly circumvented when the authorities decided to block the ‘Pirate Bay‘ website. Only a few days later, the Labaia.org alias was created and the website accessible again;
- France: The ‘AAARGH’ website is still available under more than ten different addresses albeit the fact that the High Court of Paris ordered its blocking in 2005 [5];
- United Kingdom: In 2008, as a result of an attempt to censure some content of the Wikipedia website, the free encyclopedia was totally blocked by mistake to an estimated 95% of residential Internet users during weeks [6];
- Europe: In 2010, the American government tried to censure WikiLeaks for a couple of months but hundreds of mirrors (websites identical to the original one) quickly appeared [7]

2.1. Domain Name System (DNS) filtering

DNS in few words : in order to access a website, rather than having to write the full IP address (which is actually the ‘location’ where the content really is on the worldwide network), it is possible to use a domain name. A domain name is an alias to an IP address, and an IP address can have an unlimited amount of aliases. A domain name looks like http://amnesty.org. To ensure that these aliases work, someone or something has to have a matching table that associates a precise domain name to a specific IP address, these are the DNS Servers. Anybody can install his own DNS Server and use it instead of the one provided by his or her Internet Service Provider (ISP) by default.

The following example assumes that an Internet user wants to visit the web site of Amnesty International, which is located at http://amnesty.org:

Step 1: The Internet user opens a web browser and types ‘amnesty.org’;
Step 2: (This step is hidden to the Internet user) The browser asks the DNS servers ‘which IP address is associated with amnesty.org ?’;
Step 3: (This step is hidden to the Internet user) The DNS server checks its matching table and, if a match is found, it answers by giving the associated IP address ‘195.234.175.160’;
Step 4: (This step is hidden to the Internet user) The browser contacts the given IP address and tries to access its content.

DNS blocking occurs at **Step 3**. Instead of answering the real IP address which is associated to the given alias, the DNS Server answers with another IP address which is, in most of the cases, owned by a governmental service such as the police.

There are many technical facts that makes DNS filtering (or blocking) inefficient:

First of all, when an alias is blocked, the content remains available through its IP address. If, in the first step of our example, the user types the IP address rather than typing the alias, the steps 2 and 3 will be skipped and the browser will directly contact the right server and ask for content. Therefore, DNS blocking does not work.

5. https://secure.wikimedia.org/wikipedia/en/wiki/Association_des_anciens_amateurs_de_r%C3%A9cits_de_guerre_et_d%27holocauste
6. http://en.wikipedia.org/wiki/Wikipedia:Administrators%27_noticeboard/Major_UK_ISPs_reduced_to_using_2_IP_addresses
7. https://www.nytimes.com/2010/12/06/world/europe/06wiki.html?_r=1&hp

Secondly, when an alias is blocked, the content remains available through potential other aliases. As previously said, a website can have an unlimited amount of aliases (domain name), and a domain name may easily cost less than 5 euros a year. So, it would be impossible to block every single domain name since the very low economic cost allows to have a huge amount of aliases. Therefore, DNS blocking does not work.

Thirdly, regardless the existence of aliases or the possibility to access a website using its IP address, no one should have to (and should not be forced by law to do so) use the DNS Servers provided by ones' ISP. It is a known fact that DNS Servers provided by third parties are often faster than the default ones. Moreover, it is common and easy to change DNS Servers to OpenDNS or Google's ones for instance. If, in the Step 2 of our example, one uses a third party DNS Server rather than using ones' ISP default DNS Servers, the answer received is then always the real associated IP adress. Therefore, DNS blocking does not work.

It should be noted that other means (such as VPNs/Tor network, etc.) allow to circumvent DNS filtering, which we will describe below. There again, DNS blocking is made inoperative.

2.2 Internet Protocol (IP) blocking

IP in few words : in order to access a website, a web browser has to contact the IP adress (which is actually the ‘location’ where the content really is on the worldwide network) of the server that hosts the specific website. This process is hidden to the Internet user who, in most of the cases, uses an domain name (alias) such as ‘amnesty.org’. Aliases exist due to DNS Servers providing matching tables that associate a precise domain name to a specific IP address. An IP address is like an address in a street, it means for instance ‘in this street, between the number 40 and 44, there is a building (regardless that it is a house or a skyscraper) with the number 42’. An IP address is associated to one server and may host one or many websites that are not related to each other.

The following example assumes that an Internet user wants to visit the web site of Amnesty International, which is located at http://amnesty.org:

Step 1: The Internet user opens a web browser and types the address ‘amnesty.org’;
Step 2: (This step is hidden to the Internet user) The browser asks the DNS servers ‘which IP address is associated to amnesty.org ?’;
Step 3: (This step is hidden to the Internet user) The DNS Server checks its matching table and, if a match is found, it answers by giving the associated IP address ‘195.234.175.160’;
Step 4: (This step is hidden to the Internet user) The browser asks the ISP to connect it to this IP address;
Step 5: (Tthis step is hidden to the Internet user) The ISP forwards the query to Amnesty International's server via Internet transit services and carriers;
Step 6 : (This step is hidden to the Internet user) Amnesty International's server responds by sending data packets to the user's computer and a connection is created.

For each information exchange between the user's computer and Amnesty International's server, step 5 and 6 are repeated.

IP blocking occurs at **Step 5**, instead of forwarding user's packets to destination, the ISP checks if the IP address is censored or not and carry the packet or not. If the connexion is dropped, the website or service is not accessible to the user.

There are many simple means for end users and gambling service providers to circumvent IP blocking:

On the end user side, this can be easily achieved by asking a different service (not the ISP) to create the connection, i.e. by using a so-called 'proxy'. In contrast to what is widely believed, not only experts can circumvent filters and blocking: there are many online anonymous proxies, such as http://zend2.com that allow users to simply type in the address of the blocked website in order to access it. The TOR Browser, an anonymity network browser, is another example of a popular tool that is easy to install and that allows Internet users to browse the web without any restrictions. Therefore, IP blocking is not efficient.

Based on the 'proxy' principle (ask someone else than the ISP to forward the connexion), the already widespread use of Virtual Private Networks (VPN) is another example of how IP blocking is made totally inoperative. A VPN is an encrypted tunnel between the end user and a private server, this solution is widely used whether by small companies, big corporations or universities to ensure that nobody (not even their ISP) can spy on their communications. But it can also be an encrypted tunnel to a private server that is out of the jurisdiction that the user wants to escape from. Since every single bit of the communication is encrypted, nobody can (not even the ISP), know where the tunnel exits or what kind of data transits. Therefore, IP blocking is not efficient.

It should be noted that, as said in the introduction, a specific IP address (server) can host an unlimited amount of websites or services that are not related to each other. Exactly like a skyscraper can host many companies or individuals that are not related to each other. IP blocking leads to a significant risk of collateral damage since blocking of an IP address to censure a specific website/service also discriminates every single website/service that is hosted on the same server. Therefore, IP blocking infringes fundamental rights.

2.3 Other filtering methods

Even hybrid filtering (DNS filtering and IP blocking applied at the same time) methods are not flawless, can be circumvented by any of the mean described above and suffers from the exact same lack of technical effectiveness.

Regardless of the method that is applied to try to block or filter a website, even by using the techniques that will be developed in the future, the Internet was built to offer a great level of resilience and recent cases (i.e. WikiLeaks) tends to prove that all the techniques that allows a maximum degree of resilience are widely known and easy to implement.

Web site mirroring is an example of such a technique. It can facilitate access to content on the Internet that is initially restricted. A mirror duplicates the content of a web site on another web hosting service by using a different domain name. This duplication can even consist in an automatic synchronisation of the content on all mirror sites. One of the best known examples of such a situation is what the website WikiLeaks did last year. Due to an attempt by the US government to censor the website, more than 1000 mirror sites were created within a week.

(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?

3. Unintended consequences

IP blocking measures tend to cause enormous collateral damage. Whenever a range of IP addresses is being blocked, it is very likely that other services might be unintentionally affected. Since each IP addresse can also potentially be shared by several websites, there is a risk of collateral filtering of additional unrelated Web sites. Many domains are accessible under the same IP address since the year 1999. In order to save resources, 'IP sharing' or 'virtual hosting' is very common today. Therefore, it is almost impossible to rule out unintended blocking of websites with entirely legal content.

As shown above, there is thus a risk of 'overblocking'. Even the most precise technology, such as hybrid filtering method used in the United Kingdom the so-called 'Cleanfeed' method, is not without flaws leading to the filtering of legal websites, as shown by the accidental filtering of the website Wikipedia in 2008 [8] or the blocking of 84.000 legal website by mistake in the USA recently[9]. Therefore, such measures are incompatible with the European Court of Human Rights' doctrine of 'proportionality'.

By introducing such measures, there is also a risk of the creation of a censorship infrastructure in Europe. In Italy, for instance, web blocking has first been introduced for copyright related infringements but is now being more and more extended and since July 2011, even a perfectly legal proxy site was censored.

Since blocking measures are not effective, as shown above, there is also a great danger that the introduction of the proposed measures opens the way to the development and use of more effective and even more invasive technologies, such as Deep Packet Inspection. Due to the lack of efficiency, more sophisticated means of blocking content deemed to be illegal could be introduced. However, in the long term users might develop technologies to them circumvent — a prospect which worries cyber security forces.

What is more, the introduction of web blocking and filtering systems might increase the market for the surveillance and censorship technologies. Already today, technologies developed and produced in the Western countries are contributing to censorship in authoritarian regimes. A report from March 2011 found that at least nine Middle Eastern and North African state censors use Western-built technologies to impede access to online content [10].

8. http://en.wikinews.org/wiki/British_ISPs_restrict_access_to_Wikipedia_amid_child_pornography_allegations
9. http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/
10. http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

4. Web blocking measures violate fundamental rights

The NURPA does not consider the above mentioned methods to have any merits.

On the contrary, the deployment of a web blocking and filtering system would restrict European citizens' freedom of expression and of information.

Directive 2009/140 states that restrictions to the access to the internet 'should be in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms' and that they 'shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms' [11]. The European Court reiterated the importance of freedom of expression as one of the preconditions for a functioning democracy. Therefore, even if a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued [12]. Furthermore, according to European Court jurisprudence, any restrictions need to be necessary in a democratic society [13]. However, blocking access to the websites of foreign or unlicensed gambling services that redirects users to licensed websites is neither a proportionate nor a necessary measure in a democratic society since it does not seem to protect users from their 'gambling addiction'.

The Green paper suggests the implementation of blocking measures without the involvement of an impartial regulatory body or a court order. ISPs would have to police the Internet which makes regulation less predictable and less democratic – the right to communication will be limited without any legal basis. This would result in private companies becoming a sort of censorship authority. However, the European Court notes that the most important requirement of Article 10 of the European Convention on Human Rights is that any interference by a public authority with the exercise of the freedom of expression should be lawful. The second paragraph of Article 10 clearly stipulates that any restriction on expression must be 'prescribed by law'. Voluntary blocking mechanisms and agreements as well as self-regulation mechanisms would clearly be in breach of Article 10.

The NURPA is opposed to the increase of Internet service provider liability or other 'intermediary liability' with regards to the blocking of illegal or unauthorized betting services. We are therefore against proposals that could circumvent the exemptions for 'mere conduit' provided to technical intermediaries by the E-Commerce Directive, violate the principle of network neutrality or turn telecommunication providers into watchdogs or a 'private digital police'.

Instead, the European Commission should uphold Article 15 of the Electronic Commerce Directive which prevents Member States from imposing on internet intermediaries a general obligation to monitor the information they transmit or store. The NURPA recommends that the European Commission preserves limitations on liability for Internet intermediaries.

11. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF
12. Bladet Tromsø and Stensaas v. Norway [GC], no. 21980/93, ECHR 1999-III
13. Sunday Times v. UK (No. 2), Series A No. 217, 26.11.1991, para. 50; Okçuo_lu v. Turkey, No. 24246/94, 8.7.1999, para. 43.

It should also be noted that the United Nations has said very recently that access to the Internet is a human right. Special rapporteur Frank La Rue dedicated an entire chapter of this report to the danger of blocking [14] and stressed the following (p. 10):

'Firstly, the specific conditions that justify blocking are not established in law, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body.'

The OSCE report, published in July 2011, mentions as well that

'Everyone should have a right to participate in the information society and states have a responsibility to ensure citizens' access to the Internet is guaranteed.'

Concerning blocking systems it states (p. 21):

'There is concern that voluntary blocking mechanisms and agreements do not respect due process principles within the states in which they are used. In the absence of a legal basis for blocking access to websites, platforms and Internet content, the compatibility of such agreements and systems with OSCE commitments, Article 19 of the Universal Declaration and Article 10 of the European Convention on Human Rights is arguably problematic.'

In its Green paper the Commission suggests furthermore that the blocking system will depend on a pre-defined and updated list of items to block. However, if the blocking list cannot be published, it means proper transparency and safeguards will be impossible.

14. United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011.
http://nurpa.be/resources/downloads/20110516_ONU-report-protection-promotion-freedom.pdf

Conclusion

The proposed measure to restrict and block ‘unauthorised’ and cross-border online gambling services is yet another overzealous attempt to introduce control and censorship of online communications in the EU's democratic Member States.

This attempt tries to impose an EU-wide blocking infrastructure and thus would clearly undermine fundamental rights and the European Union's voice on freedom and democracy in the world. Such an infrastructure would thus be clearly disproportionate and seems to be an ‘easy solution’ instead of trying to put more efforts into the prevention of gambling addiction, fraud and money laundering.

As shown above, filtering sites is not only an inefficient but also a dangerous measure as it might allow for an extension from gambling sites to other types of sites later on. Blocking measures could open the door to limitations of the freedom of expression and bring forth the risk of censoring the Internet.

Today, access to the internet is fundamental tool for enabling free speech. Blocking measures must comply with the European Convention on Human Rights and European Charter of Fundamental Rights, both of which require a legal basis for restrictions on fundamental rights.

We would welcome the opportunity to discuss the elements of our position on the Commission's Green Paper in more detail with the Commission, the European Parliament and Member States.

You can contact us at: contact@nurpa.be

Thank you for your consideration.

This document is available online at
http://nurpa.be/resources/downloads/NURPA_20110731_online-gambling-consultation.pdf