The Response of Access to:

Green Paper on on-line gambling in the Internal Market

SEC (2011) 321 final

JULY 2011

Table of Contents

Introduction

Access is a global movement premised on the belief that political participation and the realization of human rights in the 21st century is increasingly dependent on access to the internet and other forms of technology. Founded in the wake of the 2009 Iranian post-election crackdown, Access teams with digital activists and civil society groups internationally to build their technical capacity and to help them advocate globally for their digital rights. Access provides thought leadership and practical policy recommendations in the broader field of internet freedom, and based on that expertise mobilizes its global movement of citizens to campaign for an open internet accessible to all. We thus 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.

Access supports the Commission's initiative to address gambling addiction in the EU and to combat fraud and 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 to shared European values to see the Belgian state, for example, willfully failing to protect consumers from allegedly fraudulent TV gameshows[1] while, 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 measures must be avoided, as Access believes strongly that the design and implementation of policies in this area should reflect a citizen-centred approach.

Questions:

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 online gambling services.

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.

(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 effectiveness is broadly identical to DNS blocking. From this point forward in this document "IP blocking" will be understood as the former technology, namely, blocking of IP access *to* specific IP addresses by their consumers.

With regard to these two questions, Access' 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 is divided into four parts: (1) Effectiveness of IP Blocking and DNS-based blocking, (2) Legality of IP Blocking and DNS-based blocking, (3) Legality of IP Blocking and DNS-based blocking through non-legislative measures, and (4) Threats IP Blocking and DNS-Based blocking pose to the integrity of the internet.

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 easily IP Blocking and DNS-based blocking can be circumvented.

First, there are online proxy websites, where a user can simply input the URL (e.g., 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 is actively encouraged by the European Commission[3]) 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.[4] 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 realising 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), in addition to being "necessary in a democratic society" (Article 10) 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. In an adult population of approximately forty million (and assuming "millions of redirections means at least two), this equates to approximately a minimum of 5% of the adult population hitting the blocking system every week, or 2.6 hits per adult per year!

This statistic is quite obviously implausible and can be explained by the following reasons. Firstly, a consistent figure of millions of redirections every week could be explained by the ease of access to foreign gambling websites that, week after week, millions of Italians are not discouraged away by encountering 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.

Another reason for the high level of search engine traffic on the Italian blocking page is that this page is widely referenced on the web – according to Google, there are 1,650 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.

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF

[4] For example: http://www.youtube.com/watch?v=3ktvww9zFas&feature=related

Additionally, approaches that call for IP and DNS-based blocking do not adequately address the reality of today's internet, as static sites hosting illegal material are less and less frequent. Indeed, given the ability of websites to change location and domain with great frequency and ease makes it practically impossible to keep any filter up to date.

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 and contents 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 technology 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 reinforced if the DPI were then to be reused for anti-competitive practices, such as blocking of legal services that were in competition with the access providers' services.

Legality of 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,[5] most websites 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 automatically, blocking large numbers of innocent websites.

Such instances have already occurred in the US, where the Department of Homeland Security (DHS) accidentally seized the domain of a large DNS provider in an effort to target ten websites accused of selling counterfeited goods or hosting child abuse material. The collateral damage was disproportionate to the stated aim as 84,000 unrelated websites were taken offline.[6]

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

[5] http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/
[6] http://yro.slashdot.org/story/11/02/16/2239245/US-Govt-Mistakenly-Shuts-Down-84000-Sites%22%20%5Ct%20%22_blank

to circumvent – even accidentally. Indeed, the European Commission itself accidentally circumvented the planned blocking of gambling sites in Belgium because the computer equipment (DNS servers) it uses to access the internet is based in Luxembourg.

Deep Packet Inspection is one of the most invasive and counter-productive method of blocking access to specific content in use today. It is exceptionally privacy intrusive and would entail significant collateral damage for the functioning of the access provider and online services market in Europe.

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

1. *To protect tax revenues*

Access believes that this aim is not proportionate to the combined negative societal impact caused by the introduction of technologies to restrict access to communication, the inevitable "mission creep" to blocking other content, such as to protect copyright, and the "technology creep" to more "efficient" technologies, such as Deep Packet Inspection (DPI). Such a restriction is therefore clearly not "necessary in a democratic society" as required by Article 10 of the European Convention on Human Rights (ECHR).

The protection of tax revenues, while a legitimate aim, will not be solved by the implementation of a blocking regime in the EU. The online environment does complicate some aspects of trade, particularly as companies, or in this case, online gambling sites, can operate in several jurisdictions simultaneously. However, other nations, such as the US, have addressed this issue by imposing a Streamlined Sales Tax[7] system, which guarantees that "remote sellers" collect tax on sales from customers living in the Streamlined states, effectively levelling the playing field.

2. *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" *and* if less restrictive options, such as efficient cooperation with payment service providers or the use of effective trustmark schemes proved ineffective.

[7] http://www.streamlinedsalestax.org/index.php?page=faqs

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.

3. *As a general consumer protection measure, such as to protect citizens from gambling addiction.*

Here again, blocking would only be legal if the size of the problem made such a policy necessary in a democratic society 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 mandate 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 begin to be adequately addressed.

Access urges the Commission to address such problems as gambling addiction at its source, as filtering licit and illicit gambling sites are not an effective remedy for this societal ill. Harmful behaviours such as gambling addiction should be addressed as any other illness in the offline world – through education, parenting and support. Restricting access to such sites will only push gamblers further underground, making it even harder to identify and provide treatment to those who require it.

None 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, Access urges the Commission to repeal all existing web blocking systems that currently exist in Europe.

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 only 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 about people encountering the blocking system for child abuse material,

which explained that "it is clear that genuine ISP customers are inadvertently accessing such material."[8]

In short, 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 in May of 2010, a member of the current College of Commissioners, Comissioner Malmström, gave a strong undertaking to oppose blocking in any context outside child exploitation, stating unequivocally 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*." [9]

The illegality of blocking can also be also be adduced from Advocate General Cruz Villalón's Opinion[10] 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 the Advocate General, in order to be permissible, such a measure must comply with the conditions laid out in the Charter of Fundamental Rights to govern restrictions on the exercise of rights. With regard to these conditions, 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 fulfil 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 filter very quickly came to be used for an ever-growing range of content (4,771 sites are currently blocked). Recently, a system has been introduced to block sites in the absence of a court order, which undermines the rule of law and free speech. Completely legal virtual private network services are now also being blocked (due to fears of

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

9 http://www.meldpunt-kinderporno.nl/files/Biblio/Speech-Malmstrom-Combating-sexual-abuse06_05_2010.pdf

10 http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10

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 infringements. Long term experience in an overwhelming majority of EU countries that have introduced blocking shows that it always has unpredictable side-effects, which 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 IP Blocking and DNS-based blocking through non-legislative measures

Discussions on internet regulation in general, at nation-state, regional, and global levels are increasingly leaning towards “self-regulatory” measures and away from those that require a legal basis, as illustrated by the Italian example above. However, IP blocking and DNS-based blocking through non-legislative measures are 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 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 and sexual exploitation of children and child pornography, repealing Framework decision 2004/68/JHA.[11] In the particular text, the Commission assessed 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, Access would like to draw attention to the report[12] 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.[13]

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

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

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

Threats IP Blocking and DNS-Based blocking pose to the integrity of the internet

As we have described in some detail throughout this paper, filtering measures such as IP or DNS-based blocking are not only ineffective in achieving their stated goal (i.e. preventing access), but these approaches are a clear breach of established EU acquis, as outlined in the EU Charter of Fundamental Rights and the EU Convention on Human Rights. Furthermore, if such measures to restrict access through filtering were implemented, this would pose a substantial threat to the global DNS system, which would damage the integrity of the internet.

As DNS filters can easily be evaded, such widespread circumvention would threaten the security and stability of the global DNS.[14] With the exception of countries like Iran and China, there is relatively little censorship occurring in the global Domain Name System (DNS). However, if more countries – and the EU in particular – were to start exercising control over critical DNS infrastructure, there would likely be a flood of users shifting to alternative (uncensored) DNS mechanisms.

If such a migration were to take place, the inconsistencies between the official DNS and these censorship-free alternatives would damage the integrity of the internet, causing a number of problems including:

- causing non-blacklisted websites to be unreachable at various times due to propagation delays;
- making it harder for CDNs to send their clients to the right server
- increasing internet backbone costs by at least 20%
- causing a variety of other cybersecurity breakdowns including creating real problems for the development of DNSSEC.[15]

Conclusion

Access believes that:

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

[14] http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf
[15] https://www.eff.org/deeplinks/2010/11/case-against-coica

- Blocking potentially 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 not intended to be restricted. 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;
- Blocking through non-legislative measures (whether "voluntary" or imposed by non-judicial authorities) is contrary to Article 10(2) from the European Convention on Human Rights, which requires 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;
- Deep packet inspection is disproportionate and breaches both article 8 and 10 of the European Convention on Human Rights;
- Restrictions must not be imposed "by proxy" using intermediaries coerced into action by a intermediary content liability regime;
- Imposing filtering regimes, such as DNS blocking, poses serious dangers to the integrity of the internet, and should thus be avoided;
- Measures which prevent access to gambling sites, for the purposes of collecting tax revenues, the prevention of fraud/money laundering, and/or to combat gambling addiction are not proportional to the negative societal impact that would be caused by the introduction of technologies to restrict access to communication, such as the inevitable "mission creep" and "technology creep", and such restrictions are not "necessary in a democratic society" as required by Article 10 of the European Convention on Human Rights (ECHR)

For more information, please visit www.AccessNow.org or contact:
Access Policy Analyst Jochai Ben-Avie, jochai@accessnow.org