PUBLIC CONSULTATION ON THE GREEN PAPER ON ON-LINE GAMBLING IN THE INTERNAL MARKET
AUGUST 2011

EuroISPA welcomes the opportunity to contribute to the discussions on online gambling in the Internal Market. Our contribution will focus on the technical measures to restrict unauthorized and cross-border on-line gambling services (questions 50 and 51 of the questionnaire).

As a preliminary remark, EuroISPA believes that technical enforcement through blocking or filtering techniques will always shift the problem instead of resolving it. No technical measure has proven or is likely to be efficient, because they are not only easy to circumvent, but also inaccurate. The implementation of these techniques also entails an increase of costs to be borne by Internet Service Providers (ISPs), without any guarantee that such techniques will not become quickly obsolete in the fast moving technological world of the Internet. Above all, these additional costs generate a chilling effect on investment and innovation.

EuroISPA furthermore fears that by implementing blocking or filtering techniques, the security of the Internet will be compromised and unintended consequences outside the scope of the real problem will be generated. Indeed, any such invasive intervention affects all data (not only unlicensed gambling services) transmitted over a network and would inevitably produce a negative impact on the secrecy of communications, breaching privacy and business confidentiality.

1 SHORTCOMINGS OF DNS FILTERING

While EuroISPA supports Commission's goal of preventing the exploitation of consumers by unregulated and unsafe gambling operators, our association wishes to express important technical and security concerns with the proposed technique of DNS filtering:

- **A minimally effective technique:** DNS filtering does not prevent access to Internet content and is known to be very easy to circumvent. Some examples are as follows:
    - Users can use non-filtered DNS servers located in third countries, e.g. by using a proxy abroad or by changing their DNS settings. It is important to note that malicious websites can automatically, silently and permanently change the DNS settings of a user who visits the site to avoid DNS filtering.[1]
    - Operators of infringing sites can operate alternative DNS servers for their users.
    - Many paid and free DNS servers exist on the Internet that can give answers without filtering queries.

[1] S. Crocker, D. Dagon, D. Kaminsky, D. McPherson and P. Vixie, "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill", http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf, p.8.

- Finally, the easiest way to avoid DNS blocking measures is just to type the IP address of the blocked website into a browser's address line. PCs can easily be configured so that users do not have to remember this number at each visit.[2]

- **Circumvention methods pose serious security and performance threats:**

  - First, we would like to point out that the circumvention methods listed above expose users to increased cyber security threats. Indeed, both users and operators of infringing websites are likely to respond to DNS filtering by re-directing users' DNS settings to third country servers. In doing so, traffic could be pushed to potential rogue servers, with the consequence that infringement sites could, under certain conditions, gain access to all DNS traffic of the user and exploit thus gained access to sensitive communications[3]. This generates risks of which users may not be aware because, as mentioned above, they might not even be aware of the fact that their DNS settings have been changed.

  - Secondly, ISPs will lose visibility into network security threats as users increasingly turn to other DNS servers to avoid the DNS filtering. ISPs will be less able to identify computers that have become under the control of a criminal botnet.

  - Finally, routing DNS traffic to offshore servers affects network performance and increases costs for ISPs, especially for content delivered from Content Distribution Networks (CDNs).[4]

- **Incompatible with DNS Security Extensions (DNSSEC)**: The quick pace at which new technologies such as DNSSEC develop, will render DNS blocking quickly obsolete. Indeed, redirecting users to a resource that does not match their request (i.e. when a user is redirected from a blocked website to a so called stop-page), is the very behavior that end-to-end DNSSEC is designed to detect and suppress. Although today DNSSEC-enabled applications are not yet widespread, their deployment is expected to grow due to the fact that sensitive applications, such as online banking and e-health, are becoming more effectively and efficiently secured.

- **DNS-blocking is limited to the networks of Internet Access Providers**: DNS-blocking is efficient only when the request to access a website passes directly through the DNS server of an Internet access provider. However, many entities such as public and private companies, universities, hospitals dispose of their own DNS servers. This implies that the implementation of DNS filtering would require addressing all such entities as well.

- **Possible side effects**: the introduction of DNS-blocking would promote the development of circumvention techniques. The DNS system, however, has been one of the most important enablers of the innovation and economic growth generated by the development of the Internet. Indeed, by providing universal domain names, DNS makes the Internet the unified global communications network that it is today[5]. The indirect promotion of circumvention techniques would inevitably modify the same nature of the Internet architecture in a way that is difficult to predict.

- **Collateral damage by 'over-blocking'**: DNS blocking implies blocking the entire domain name at the level of a DNS server. This means that if illegal games of chance are hosted on a subdomain, all other (legal) subdomains that have the same parent

[2] Idem, p. 9.
[3] Idem, p. 11.
[4] Idem, p. 12.
[5] Idem, p. 4.

domain will be blocked as well. This would have a direct impact on the freedom of communications, especially because the existence of additional subdomains may not readily be apparent[6].

- **Increased costs of monitoring:** the re-direction to another (legal) site is a signal for illegal operators to move their website to other servers abroad. We are already experiencing in relation to the child sexual exploitation fight that the adoption of DNS blocking has the consequence to reduce the time laps between the blocking of a website and the appearance of a new one with the same content. This would inevitably increase the costs related to the monitoring of illegal websites online and make enforcement less effective and economically burdensome.

- **Jurisdiction problems:** An ISP can locate its DNS server in one Member State and use that server to also provide services in other Member States. Given that DNS blocking always applies to the entire server, a website that is illegal in one Member State will also be blocked in other Member States where it might not be illegal. This makes it impossible for an access provider to comply with diverging gambling legislations of different Member States of the Single European Market in which it may offer its services.

For all these reasons, **EuroISPA considers DNS blocking to be minimally effective, risky in terms of security, costly in terms of monitoring and to present important side effects.** Furthermore, EuroISPA wishes to stress that the fact that millions of users are being re-directed every day in countries where DNS blocking is applied, does not in any way imply that these users are effectively being brought to play on the legal gambling market, especially if illegal gambling offer is more attractive.

2 SHORTCOMINGS OF IP BLOCKING

IP blocking is a second technical measure that could be imposed on ISPs to prevent all traffic from routing to specified IP addresses. This method, however, presents severe shortcomings:

- **Very high risk of over-blocking:** most websites share IP addresses, therefore the blocking of an IP address would almost automatically block large numbers of other (legal) websites. This high level of over-blocking, due to shared web space (e.g. all of MySpace, Geocities, terra.es, etc.), would inevitably generate economic damages for e-commerce providers.

- **Circumvention:** although IP blocking is less easy to circumvent than DNS blocking, it is still possible using tunneling and virtual private network (VPN) tunneling techniques. Tunneling allows users to create an encrypted “tunnel” to a different machine on the Internet, which prevents the filtering software from seeing web requests. VPN tunnels are invariably encrypted and thus not susceptible to interception.

- **Using Anonymous website**: There are many websites that allow surfing the Internet anonymously. Some of the websites provides options for encrypting the URL’s of the websites. These proxy websites will hide the IP address and will show another IP address which would prevent the website being blocked, making it easy to access it.

- **Possible side effects**: given that IP blocking is circumvented through encryption, the implementation of such a system may promote the encryption of the networks, thus pushing illegal online gambling activities into clandestinity.

[6] Idem, p. 13.

An IP blocking system, when applied at ISP level, would unavoidably lead to a large amount of legal content being blocked. Besides their intrinsic, technical inefficiency, such system is also disproportionate in the field of online gambling. **EuroISPA believes that if a system of IP blocking were ever to be implemented, this could most efficiently be done at the level of the gaming operator, which could indeed block IP addresses of countries where the gaming operator has no license to provide services.** The involvement of ISPs could in that case be avoided and the risk of over-blocking minimised.

3 CONCLUSION

At EU level, many Member States have raised regulatory barriers in order to prevent foreign operators from offering gambling services to their citizens, whether by strictly controlled monopolies or by limiting the number of available licenses. However, the growth of the Internet has allowed operators of gambling services to overcome such barriers and reach consumers in countries where they are not legally licensed. The implementation of technical measures did so far not help solving the problem of gambling sites hosted abroad remaining accessible. On the contrary, such measures risk to compromise the security of the Internet and to generate unintended consequences outside the scope of the real problem. EuroISPA supports the emergence in the EU of a legal framework for online gambling, but remains skeptical about the effectiveness and proportionality of the technical measures used or advocated.

EuroISPA *is the world's largest association of Internet Services Providers (ISPs) representing the interests of more than 1800 ISPs across the EU and the EFTA countries. EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet (www.euroispa.org). Contact: Andrea D'Incecco, Head of Policy (+32 2 503.22.65/ andrea@euroispa.org).*