BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Stichting Bits of Freedom
PO Box 10746
1001 ES Amsterdam
The Netherlands

M +31(0)6 5438 6680
E ot.vandaalen@bof.nl
W www.bof.nl

Bank account 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

European Commission
DG Internal Market and Services
markt-gambling@ec.europa.eu

Re:
Consultation on the Green Paper on on-line gambling in the Internal Market

Date
Amsterdam, 31 July 2011

Dear sirs,

1. The Dutch digital rights organisation Bits of Freedom ("**Bits of Freedom**") would like to take this opportunity to respond to the public consultation of the European Commission on the Green Paper on on-line gambling in the Internal Market (the "**Paper**"). Bits of Freedom defends freedom and privacy on the internet. We will consequently focus on questions 50 and 51 of the consultation, which concern the application of so-called "Domain Name System (DNS) filtering" and "Internet Protocol (IP) blocking".

> *"(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?*
> *(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?"*
>
> For the sake of clarity, we understand these terms to mean the blocking of access to websites at the access provider, and not the serving of different websites to different visitors, depending on the IP-address of the visitor.

2. It is difficult to provide a useful answer to these questions in the abstract, without – for example – having more knowledge about the policy goals underlying each of these measures, the problems which need to be solved and the alternative measures available. In general, however, the application of these technologies always should be considered a restriction on the freedom of expression as set out in Article 10 of the European Convention of Human Rights ("**ECHR**") and Article 11 of the Charter of Fundamental Rights of the European Union ("**Charter**"). Such restrictions need to be subject to a rigorous analysis, involving multiple considerations, which – with the current evidence available in its Paper – lead to the conclusion that the application of DNS-blocking and IP-blocking should be considered a violation of these rights.

- **Goals**. For two reasons, it is essential to investigate which policy goals underlie specific restrictions on on-line gambling. Firstly, as indicated by the European Commission in its Paper, consumer protection and the prevention of money laundering could be considered aims which may justify a restriction under Article 51 and 52 Treaty on the Functioning of the European Union. The protection of tax revenue, however, cannot be considered an interest recognized under these provisions. Similarly, Article 10 ECHR and Article 52 of the Charter do not recognize the protection of tax income as a legitimate aim.
  Secondly, it is essential to investigate the policy goals which underly each specific restriction, because each restriction will have to be 'necessary in a democratic society' (as set out in Article 10 ECHR). This involves an analysis of proportionality and subsidiarity, which implies that the goals need to be as clear as possible.
- **Necessity**. It should further be noted that the requirement that each measure has to be 'necessary in a democratic society', is very strict. This means that there needs to be convincing evidence that this restriction corresponds to a pressing social need.
- **Effectiveness.** The technology applied in DNS- and IP-blocking is very easy to circumvent. In fact, the United States and the European Union are actively developing technology to facilitate circumvention, in order to allow citizens in Iran and China access to politically sensitive information in these countries. These technologies can and will also be used in the European Union. There are numerous videos available on the web which explain how such restrictions can be circumvented. Obviously, if restrictions can be circumvented easily, it is difficult to see how these measures can be considered an effective way to reach any of the legitimate aims discussed above.
- **Proportionality**. Each restriction needs to comply with the requirement of proportionality. This means that the measure does not go further than necessary. Restricting access to websites by way of DNS- and IP-blocking implies that there is an intention to make an *entire* website unavailable until the block is lifted. This means that all services which may be offered on the same website which are considered lawful under the state which imposes the access restriction, are also made unavailable to the citizens of this state. This is even more far-reaching in those cases where IP-blocking would be applied and several websites use the same IP-address (which is then redirected to the required website depending on the name of the website the user is visiting). Restricting access to an entire website thus in most cases will be a disproportional measure. More fine-grained measures, restricting access to only certain services or parts of a website will involve a detailed analysis of all internet traffic of all internet subscribers, and are consequently a disproportionate infringement on the right to privacy.
  Another consideration in the context of proportionality is the fact that any system in place for restricting access to online gambling services or websites can be used for the restriction of access to other types of websites as well. The potential for function creep needs to be kept in mind when analyzing proportionality.
- **Subsidiarity**. Each restriction in addition needs to comply with the requirement of subsidiarity. This means that there are no other, less restrictive measures which achieve the same goal. In the context of the prevention of money laundering, it for example would have to be investigated to what extent the extant rules and regulations regarding money laundering are sufficient to address this problem. In

the context of consumer protection, it for example would have to be investigated what the size of the problem is, what range of measures are available to address this problem and what the effectiveness of each of these measures is.

3. It is impossible to provide further input on these questions without knowing more about the context of any measures under consideration. We trust, however, that the European Commission will apply the human rights-framework which necessarily applies to all its regulations diligently in the context of online gambling policy.

4. If possible, we would like to remain informed on the further steps of the European Commission in this field. Please do not hesitate to contact me, should you have any questions.

Sincerely yours,

Ot van Daalen