



FUNDACJA WOLNEGO I OTWARTEGO OPROGRAMOWANIA

ul. Staszica 25/8, 60-524 Poznań, www.fwioo.pl, info@fwioo.pl
tel.: +48 61 6232536, +48 61 6243474, fax: +48 61 6232504
KRS 0000277338, REGON 300545500, NIP 7811798805
BRE Bank S.A., nr rach.: 96 1140 2017 0000 4602 1136 0627

Warsaw, 30.09.2013

Questions regarding central-level Internet filtering proposal

This document attempts at gathering all the relevant questions that need to be asked and answered with regard to any proposal of introducing a central-level Internet porn censorship solution, and can be used as a map of the related issues that would also need to be decided on.

Questions herein are for the most part not deeply technical and do not require an answer containing any concrete technical solutions. They also do not touch economy-related issues.

1. **What definition of pornography is to be used in the context of the proposed solution?** In particular:
 - i. Are graphic works and animations not created via image recording techniques to be included in that definition?
 - ii. Are textual works describing sexual acts to be included also?
 - iii. Are audio materials to be included?
 - iv. Are works of art containing or presenting nudity to be included? If not, how are they going to be differentiated?
 - v. Are biology and sexual education materials to be included? If not, how are they going to be differentiated?
2. **Who is to decide on putting given content on the blocked content list?** In particular:
 - i. What oversight measures are proposed to combat instances of putting (willfully or by mistake) non-pornographic content on said list?
 - ii. Will the blocked content list be public, or secret?
 - iii. If the list is to be kept secret, what are the reasons for doing so?
3. **How is the content to be blocked going to be identified?** In particular:
 - i. Is the content identification to be based on textual keywords within content itself?
 - ii. Is it to be based on keywords in URL leading to content?
 - iii. Is it to be based on an explicit blacklist of URLs?
 - iv. Is it to be based on an explicit blacklist of domains?
 - v. Is it to be based on an explicit blacklist of IP addresses?
 - vi. Is it to be based on image recognition?
 - vii. Is it to be based on audio recognition?
 - viii. Is it to be based on checksum comparison?
 - ix. Is it to be based on a combination of methods? If so – which methods are to be employed?
4. **What remedy procedure is considered in case of blocking of content that does not fulfill the definition of pornography?** In particular:
 - i. Where and to whom such incidents are to be reported?
 - ii. What would the confirmation or denial procedure for such reports be?
5. **What remedy procedure is considered in case of not blocking of content that does fulfill the definition of pornography?** In particular:
 - i. Where and to whom such incidents are to be reported?
 - ii. What would the confirmation or denial procedure for such reports be?
6. **Are parents/legal guardians/subscribers to have control over the scope of blocking?** In particular:
 - i. Will they be able to indicate that given content should be excluded from blocking, even though it does fulfill the definition of pornography?
 - ii. Will they be able to indicate that given content should be blocked, even though it does not fulfill the definition of pornography?



FUNDACJA WOLNEGO I OTWARTEGO OPROGRAMOWANIA

ul. Staszica 25/8, 60-524 Poznań, www.fwioo.pl, info@fwioo.pl
tel.: +48 61 6232536, +48 61 6243474, fax: +48 61 6232504
KRS 0000277338, REGON 300545500, NIP 7811798805
BRE Bank S.A., nr rach.: 96 1140 2017 0000 4602 1136 0627

7. **Is the blocking solution to be opt-in, opt-out, or is the choice to be presented upon first connection?** In particular:
 - i. Is the choice going to apply to all devices using a given connection?
 - ii. Is the choice going to apply only to a particular device on any connection?
 - iii. Is the choice going to apply only to a particular device on a particular connection?

8. **Is the choice to enable blocking is to apply also to institutional subscribers and companies?** In particular:
 - i. If not, does that mean no blocking, or mandatory blocking?
 - ii. Is it to apply to libraries?
 - iii. Is it to apply to schools?
 - iv. Is it to apply to universities and other higher education institutions?
 - v. Is it to apply to public hot-spots run by local communities?
 - vi. Is it to apply to public hot-spots run by private service providers?
 - vii. Is it to apply to hot-spots provided only for private service providers' customers?
 - viii. Is it to apply to hot-spots run by private companies for their employees?

9. **Will content explaining how to circumvent blocking also be blocked?**

10. **How is HTTPS or other SSL/TLS-encrypted traffic to be handled?** In particular:
 - i. Is HTTPS/TLS/SSL traffic to be ignored altogether?
 - ii. Is HTTPS/TLS/SSL traffic to be blocked?
 - iii. Is HTTPS/TLS/SSL traffic to have encryption layer broken and content filtered?

11. **How is private communication to be handled?** In particular:
 - i. Is e-mail and Internet messaging communication to be filtered?
 - ii. Are peer-to-peer networks to be filtered?
 - iii. Are MMS messages to be filtered?
 - iv. Is private audio-video (including VoIP) communication to be filtered?
 - v. Is private audio communication via regular and mobile phones to be filtered?

12. **How is encrypted private communication to be handled?** In particular:
 - i. Is such communication to be blocked?
 - ii. Is such communication to be ignored?
 - iii. Is such communication to have encryption layer broken and content filtered?

13. **Are solutions regarding HTTPS/TLS/SSL and private and encrypted private communication to be implemented in networks operated by institutional subscribers and companies, as per question 8. above?**

Best regards,

Michał Andrzej Woźniak