The workshop began with a presentation from Andrei Robachevsky, providing an introduction of the issue of blocking content in the Internet. The scope of the workshop was limited to the content that is generally seen as illegal, without going into discussion what is illegal or not. Freedom of speech, while a very important issue, was set outside the scope of this workshop. Illegal content is a serious issue: it impedes creativity, fosters criminal activity and affects the reputation of the Internet. Therefore, removing illegal content from the Internet is an important goal. There are two main options: remove it at the source, or block its consumption. There are challenges for both approaches. First, this is a cross-border issue: the source and consumer in different jurisdictions and definitions of what's illegal may differ. Secondly, there are several trade-offs that might be affected, consider implication for privacy and security, impact on the global Internet and its innovative potential as well as the international principles of rule of law and due process.

The speaker than illustrated these concepts by providing a case in point: DNS filtering. - a proposed technical method to block content consumption. One of the advantages of this method is that it can be implemented on a national level, making DNS, one the fundamental components of the Internet, an attractive lever for policy makers. At the same time this method has serious deficiencies that significantly overweight possible short-term benefits. In fact, this protection doesn't solve the problem and can be easily circumvented, exposing users to security risks. It is incompatible with DNS security extensions -
DNSSEC, and causes collateral damage, impacting the integrity of DNS and reducing global Internet security.

Following this introduction the panelists were offered several questions stimulating discussion of different views on this problem and possible solutions.

Is non-consented blocking content at the consumption by using technical means effective?

When discussing this topic, participants shared different views on the effectiveness of the technical means and DNS blocking in particular.

None of the means are 100% effective. Some of the participants stated that DNS blocking, for example, was an expedited, simple and effective way of blocking content at consumption level. Other participants argued that this means can be easily circumvented, also pointing to the fact that it doesn't stop access to the content, but stops the ability to access the content using specific domain name. Effectiveness of the blocking also depends on how well user interests are aligned with the objectives of the blocking content.

Blocking content lacks precision. In order to be effective blocking should be focused and precise, but many of the proposed and used technical means lack that. For instance DNS blocking is very coarse and causes collateral damage.

Blocking content may have unintended consequences. Some of the panelists provided examples when blocking content may result in negative social and economic consequences, especially in the developing world, when the whole countries may be restricted to access certain content of on-line services, including ability to conduct financial transactions.

Scale and scope. Many participants raised the point that not all illegal content has same characteristics and warrants same urgency and technical means in combating it. There are extreme cases, like child sexual abuse material, that are very different both in scale (order of a few hundred domain names), and in the general public agreement that this is a serious crime, which may require all available technical means and tight control over its use. It was noted that in these cases DNS blocking helped achieving positive results, especially when accompanied by other measures, like active takedown of actual sites. At the same time people pointed out that extreme cases don't make for good policy.

What are the short- and long-term gains and losses?

When discussing this topic the participants of the workshop made the following observations:

- Blocking content may serve as an indicator to the criminals that their activity is discovered and being watched, causing them to move elsewhere and making it more difficult to trace down and attack the source. At the same time some participants noted the need to signal to the users that they might be engaging in a criminal activity.
• Blocking content stimulates development of circumvention techniques that may expose users to security risks and erode the open architecture of the Internet.

• Blocking can produce quick short-term results with diminishing returns because of circumvention. But also because blocking itself doesn't address the real problem of child abuse or piracy it cannot be effective in the long run.

• Blocking content by technical means at consumption level puts the costs of implementing and maintaining it on ISPs. These costs can be significant, especially if a service provider operates across borders and has to implement different blocking regimes depending where users reside. Blocking can also prevent ISPs from providing effective DNS service to their customers in the long term.

• Several panelists noted that addressing these problems is not an either/or solution and a comprehensive assessment of the short- and long-term benefits against the costs is needed.

What are the venues, national or international, for developing solutions?

The second part of the workshop was dedicated to discussion of what more effective solutions to these problems might be and what would be the venues for developing such solutions. This discussion revealed the following points:

It was noted that in addressing these issues all parties involved - DNS registries and registrars, IPS, web- and hosting providers, payment providers, advertisement companies and government - need to coordinate better and "gather together under the same tent" more regularly.

Several successful examples of national and international cooperation of addressing the source of the problem were presented.

• In Germany instead of blocking content, active removal of websites promoting child abuse from the Internet is being done. The results are encouraging - in two weeks in 98% of the cases illegal content was removed by the providers after the initial request from the federal criminal police.

• Example of effective international collaboration was presented by INHOPE, representing 40 national hotlines for child sexual abuse, which act according to the national protocols in close collaboration with national law enforcement. This collaboration enables quick cross-border exchange of information to facilitate effective actions on the national level.

It was also noted that because of the global nature of the Internet cooperation between different civil societies and organizations and businesses work much more efficient and faster than agreement between the governments and more efforts should be put in stimulating "horizontal" cooperation.
Many participants highlighted the importance of public-private cooperation on these issues, providing examples, like the London Action Plan.

Another area, where effective solutions could be found is ensuring support of financial and advertising intermediaries. Focusing on these intermediaries doesn't raise the same kind of security or overbreadth concerns that the DNS blocking does raise. And on the other hand focusing on the source of money for these sites, the source of their profits could be very effective.

One participant raised concern that if the public-private cooperation doesn't work effectively with the national legal system, doesn't include police or includes police that is not skilled or comes from the countries, which we do not trust for their rule of law, what is the legitimacy behind that action?

**Takeaways**

At the conclusion of the workshop the panelists made closing remarks summarizing the main takeaways for the workshop.

- For effective solutions all involved parties should be part of the development of the solution, without unnecessary duplication of efforts. These efforts should include comprehensive cost-benefit assessment of the tools, which are not necessarily technical solutions. Financial support, payment systems and advertising were mentioned as areas where such tools should be developed and applied, among others.

- "Horizontal" cooperation as well as public-private partnerships can be effective tool in solving problems of illegal content. These forms should be further enhanced and made more effective.

- The focus should be on the real problem, not symptoms. To the extent possible, the focus and direct actions must be against the bad actors themselves.

- Severity of the illegal content may warrant different approaches and toolkits.

- Blocking content may have many unintended consequences and cause significant collateral damage. In the developing world, blocking may result in "blanket" blocking, outcasting the whole communities, or countries.

- There were opposing views regarding the use of DNS for blocking content at the consumption level. By some of the participants it was seen as a quick and effective, at least in the short-term solution. Others pointed out its ineffectiveness, risks that circumvention will bring and significant costs that ISPs in particular have to incur.