IGF BACKGROUND PAPER

WORKSHOP 105: "THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES"

OECD

BACKGROUND AND OBJECTIVES

The OECD's project on Internet intermediaries follows up on the mandate given to the OECD in the Seoul Ministerial Declaration to "examine the role of various actors, including intermediaries, in meeting goals for the Internet Economy." The overall goal of the horizontal report of the OECD's Committee for Information, Computer and Communications Policy (ICCP) is to obtain a comprehensive view of Internet intermediaries, their economic and social function, development and prospects, benefits and costs, and responsibilities.

The first part of the project on Internet intermediaries, which took place in 2009, focussed on the economic and social role of Internet intermediaries in supporting the Internet economy and innovation processes. It developed a common definition and understanding of what Internet intermediaries are, of their economic function and economic models, of recent market developments, and discussed the economic and social uses that these actors satisfy. In particular, information on the Internet is distributed, hosted and located by Internet intermediaries, whose role in the structure of the information society is therefore critical. They facilitate free expression, the exchange of information and more generally drive the development of new intellectual assets, social and commercial interactions, and innovation.

The second part of the project, in 2010, focuses on public policy issues associated with Internet intermediaries, in particular, the roles and responsibilities of Internet intermediaries for actions by users of their platforms. A workshop on "The Role of Internet Intermediaries in Advancing Public Policy Objectives" was held on 16 June 2010 in Paris. It discussed and tried to identify lessons learned from experience to date of Internet intermediaries in advancing public policy objectives. It was supported by Norway and brought together about 40 speakers from the technical and academic communities, government, and the private sector (www.oecd.org/sti/ict/intermediaries). This document provides a summary of the Paris workshop of 16 June 2010. This report was prepared by Ms. Karine Perset and Mr. Alejandro Mantecón-Guillén of the OECD's Directorate for Science Technology and Industry.

The goal of the OECD/Government of Norway Workshop at the IGF, to take place on 16 september at 14:30 in Room 1 in Vilnius, Lithuania (www.oecd.org/internetgovernance), is to follow-up on the workshop held in Paris. It will more specifically discuss good practices that should be taken into account by governments when devising policies involving Internet intermediaries. The workshop will focus on the difficult but critical balancing act needed of protecting intermediary functions that are socially, economically or politically valuable, while at the same time taking into account other and potentially competing policy goals, such as protecting security, privacy, intellectual property rights or consumers.

KEY FINDINGS FROM THE EXPERIENCE TO DATE OF INTERMEDIARIES TAKING ON PUBLIC POLICY-RELATED ROLES

The OECD's project on Internet intermediaries has raised a critical question for the Internet Economy. That is, to what the extent should Internet intermediaries, which own and operate Internet platforms, be responsible for content originated by third party users? Or inversely, how far should responsibility remain with the original content author or provider, and what are the consequences for the Internet Economy? In some circumstances, Internet intermediaries are well-placed to monitor their own systems for content, transactions and activity of a certain type to help advance some public policy objectives for the Internet. They are, however, not necessarily competent to assess illegality – nor arguably should they be placed in a position where they are required to make such assessments. Internet intermediaries already engage in numerous and effective efforts to keep their platforms and services free of illegal activities. Mechanisms

used include individual business policies, industry self-regulation and co-regulation. Some of the findings from the Paris workshop follow.

Overall, there are increasing numbers of efforts to hold Internet intermediaries to duties of care, by governments and interest groups. In parallel, there is increasing pressure for intermediaries to *act ex-ante* rather than just *react ex-post*. However, the unpredictability in the application of law impedes private sector confidence. In addition, government policy initiatives involving Internet intermediaries are not always well co-ordinated and only limited quantitative information as to costs and efficiency is available.

In general, imposing liability or other responsibility on Internet intermediaries for content created by third parties can raise risks to free speech, privacy, innovation, and competition. Different opportunities and issues are raised by different implementation mechanisms such as notice and take-down schemes, notice and response schemes, technical measures, dispute resolution mechanisms and redress and education and awareness building measures. For example, processes to determine content to be filtered raise concerns related to transparency.

INITIAL GOOD PRACTICES DEVELOPMENT

The following good practices draw on the findings from the 16 June 2010 workshop. To create a policy environment that encourages the positive contributions which Internet intermediaries can make to economic and social progress and minimises legal uncertainty, governments may wish to take into account the following considerations when developing policy approaches:

1) Provide appropriate protection and liability and remedy limitations to Internet intermediaries for actions of third party users of their platforms and services, so as to enable intermediaries to help address policy objectives while at the same time encouraging growth, innovation, and the free flow of information in the Internet Economy.

2) In considering whether to adopt policies involving intermediaries, respect the following general principles:
   - Consider the role of all relevant stakeholders and involve them in the policy-making process.
   - Ensure that any policy intervention does not jeopardise needed investment.
   - Ensure that a whole-of-government approach is taken.
   - Differentiate the variety and level of Internet intermediary activities.
   - Consider whether marketplace incentives are aligned with policy goals and externalities.
   - Consider overall social cost and externalities.
   - Undertake cost-benefit analyses that assess costs and benefits to intermediaries and other affected parties.

3) Encourage and support private sector initiatives to self and co-regulation:
   - Encourage innovative private sector initiatives.
   - Encourage self or co-regulation where they hold promise to be effective.
   - Provide support for the enforcement of codes of conduct.
   - Encourage intermediaries to consider public policy objectives such as privacy, security, the maintenance of fundamental rights, and consumer protection when designing their technical and organisational systems and processes.
   - Recognise that in some cases governments have important roles to play.

4) In implementing policies and frameworks involving intermediaries, respect the following principles:
   - Determine fair and efficient arrangements for cost sharing.
   - Undertake risk assessments that evaluate unintended consequences.
   - Assess the impact of policies on civil liberties and set-up safeguards.
   - Provide for due process.
   - Protect consumers who have obtained content legitimately.
   - Reduce the need for Internet intermediaries to have to make subjective assessments of legality.

5) Co-operate with the private sector and other stakeholders to generate quantitative data.

6) Co-operate internationally.
   - Improve clarity/predictability and consistency of legal frameworks applying to Internet intermediaries
   - Consider the cross-border implications of national initiatives.
   - Increase cross-border enforcement cooperation.
   - Increase international harmonisation in some areas, bringing in the full range of stakeholders to work towards enhanced mutual cooperation and exchange of best practice.

ANNEX: DETAILED FINDINGS FROM THE OECD'S WORKSHOP ON "THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES", HELP ON 16 JUNE 2010 IN PARIS (WWW.OECD.ORG/STI/ICT/INTERMEDIARIES)

Intermediaries are increasingly important and empower end-users

As the Internet has grown to permeate all aspects of the economy and society, so too has the role of Internet intermediaries that bring together or facilitate interactions, transactions or activities between third parties on the Internet. Internet intermediaries influence and determine access to and choice between online information, services and goods. They provide tools that enable users to access information and provide new opportunities for social activities, speech and citizen participation.

Liability limitations have been instrumental in enabling the growth of the Internet

Limitations of liability for Internet intermediaries have enabled these entities and the wider Internet economy to flourish, and facilitated growth and innovation. Limitations of liability established in the late 1990s were complemented both by self- and co-regulation initiatives but also by safeguards from existing institutions and laws.

But there is an increasing number of efforts to hold Internet intermediaries to a duty of care

Participants stressed that there is increasing national and international pressure from governments, intellectual property right-holders, and some consumer groups, to enlist the help of Internet intermediaries to control copyright infringement, child pornography, improve cyber security etc. This has resulted in lawsuits from some stakeholders and court decisions that challenge existing limitation of liability regimes. Some participants noted that European courts have shown increased willingness to find that Internet intermediaries have a duty of care in some circumstances, but that these rulings have been unpredictable.

…as well as increasing pressure for intermediaries to act ex-ante rather than just react ex-post

While Internet intermediaries generally have a duty to *react* promptly to requests from consumers or governments to obtain the benefit of limitation of liability regimes, participants highlighted some open questions of whether they also have a duty to *act* in some cases, highlighting recent efforts to impose more pro-active monitoring procedures. Participants noted that some Internet intermediaries have voluntarily established *ex-ante* procedures that are manual and therefore cannot easily scale.

Unpredictability in the application of law impedes private sector confidence…

The unpredictability of some court decisions, (or not), imposing duties of care on intermediaries was felt to create considerable uncertainty among industry stakeholders.

…highlighting the need for clarification and guiding principles

Participants stressed that, in 2010, policy makers were faced more than ever with a delicate balancing act between, on the one hand, continuing to protect intermediary functions which enable economically, socially, and politically valuable activities and, on the other hand, balancing this with other policy goals, such as protecting security, privacy, intellectual property or protecting consumers. Industry agreements, as well as guidance and clarification by governments of how existing laws apply to new actors and scenarios were viewed by some participants as ways to help address uncertainties.

Fair cost distribution and due process should be taken into account

In the limited circumstances where Internet intermediaries are vested with enforcement and monitoring responsibilities, participants repeatedly stressed the importance of ensuring that the methods used are accurate, distribute costs fairly, and adhere to due process norms such as transparency, accountability and redress.

All stakeholders have a role to play in improving trust on the Internet

Participants pointed out that all stakeholders have important roles to play in improving trust on the Internet: intermediary platforms are part of an ecosystem that also includes buyers / sellers, application developers, advertisers, merchants, law enforcement agencies and users. A strong multi-stakeholder partnership was viewed as crucial to address new policy issues by incentivising the entities capable of remedying policy problems, while preserving the open nature of the Internet.

Governments should set the rules of the game and facilitate private sector initiatives

It was noted by some participants that in addition to enforcing existing laws, governments should clarify how existing laws apply to different scenarios and provide guidance for Internet intermediaries on their legal obligations. Another important role of governments was highlighted as facilitating the creation of voluntary codes and providing financial and institutional resources to support private sector efforts, for example, in the case of partnerships to improve cyber security, where examples involved: *i)* funding project set-up, threat resources centres; *ii)* ensuring transparency and due process and helping to build awareness; *iii)* providing legal tools and *iv)* convening and facilitating discussions between stakeholders.

Technical capacity alone is insufficient

Participants agreed that the technical feasibility of intermediary intervention did not provide sufficient justification for requiring it and cautioned that policy makers needed to be aware of unintended consequences. While Internet intermediaries may have the technical capacity to prevent some of the harms,

the consequences of 'deputizing intermediaries' to exercise this capacity on behalf of governments were not clear, with potential unintended consequences.

The variety of Internet intermediary activities calls for differentiation…

Several participants highlighted that a one-size-fits-all approach was inappropriate in view of the diversity of Internet intermediaries and business models. In particular, major differences were identified between Internet intermediaries in the services they offer, competition they face, nature of their consumer relationships, corporate size and entry barriers, making differential treatment necessary.

Data and cost-benefit analyses are needed for evidence-based policy-making

There was general agreement that collecting relevant descriptive data is crucial to conduct impact assessments of proposed solutions, which should include assessing the status quo, and conducting cost-benefit and risk analyses for implementing proposals. Many participants highlighted the challenge of obtaining information related to the activities of Internet intermediaries and pointed out that intermediaries may have disincentives to share information for fear that additional responsibilities might be assigned to them.

The impact of policies on civil liberties should be assessed and safeguards set-up

It was stressed that the development of applicable policy principles for Internet intermediaries should consider social development aspects, particularly human rights and democratic rights. In some cases, government policies oblige intermediaries to proactively monitor the information that they transmit, which raises concerns about the risk of content censorship and freedom of speech violations. Governments including the United States, Sweden, France and the Netherlands are investigating strategies to protect freedom of speech on the Internet. Self-regulatory initiatives such as the Global Network Initiative (GNI), that requires that its members' companies conducting *ex-ante* civil rights impact assessments are widely viewed as a best practice.

Depending on the issues, the incentives of intermediaries may or may not be aligned with public policy goals and intermediaries may or may not be in a good position to detect and address wrong-doing

The importance of thinking through the alignment of economic/marketplace incentives with policy goals and externalities was highlighted. Participants also pointed out that indirect liability can reduce overall social cost when two conditions are met: *i)* the intermediary is in the best position to detect wrong doing; and *ii)* the intermediary can internalise a negative externality – *i.e.* costs that result from decision to act (or not act), but are incurred by parties who are not responsible for the decision.

- Participants agreed that ***security*** is a common goal of stakeholders but that incentives and capabilities frequently do not align. End users are often not able to account for the third party consequences caused by their poor security practices. Security experts agreed that ISPs can help improve cyber security, although that role is fraught with risk. Japan has had positive results that Germany and Australia are also trying to achieve in setting up public-private partnerships. These partnerships involve voluntary industry codes of conduct setting up processes for ISPs to notify subscribers whose computers are suspected of being infected by malware. Security experts cautioned that imposing policy objectives on Internet intermediaries could impact competition notably by favouring large established firms, but could also generate additional security risks, because intermediaries would have to build surveillance and control systems that could invite abuse.
- In protecting ***privacy*** on the Internet, participants highlighted a conflict of interest facing intermediaries whose business model relies on monetising personal information of users as a way of

financing services offered at no direct cost. They emphasised that privacy depends on the concept of consent and that it is often impossible for Internet platforms to discern whether a person has consented or not to the material related to him/her being on the platform. Furthermore, participants agreed that on Web 2.0 platforms, it is very difficult for Internet intermediaries to differentiate personal data from non-personal data, although they are in a position technically to protect privacy, *e.g.* through strict default settings. Participants called for effective enforcement of existing legislation through improved co-operation between industry, policy makers, regulators and civil society representatives.

- Participants tended to feel that public policy goals related to protecting ***intellectual property*** rights were not necessarily always directly aligned with intermediaries' goals of encouraging platform use. Some participants argued that the involvement of intermediaries may not result in cost savings in terms of detection or of enforcement and that a proper impact assessment requires consideration of social costs and implications for due process rights. Others argued the costs were acceptable and the system provided an education opportunity. While voluntary arrangements were generally viewed as the preferred route, participants noted that in some cases government intervention was necessary to facilitate co–operation to ensure a level playing field. Innovation and attractive new consumer offers were seen as critical to encourage creativity and lawful ways of valuing creativity.
- ***The safety dimensions of consumer policy*** were viewed as an area in which intermediaries' market incentives were aligned with the objectives of policy makers, since players such as online marketplaces and payment providers have a strong incentive to meet consumers' security and payment systems concerns in order to trigger repeat purchases. In addition, these actors are often in the position to detect and deter abuses such as fraud and are making significant efforts to enhance consumer confidence. E-commerce sites and payment providers develop tools and practices to secure payment methods, fight identity theft and fraudulent activities, and offer redress mechanisms such as charge backs to consumers.

Various implementation mechanisms raise different issues

Notice and take-down schemes – whereby intermediaries set-up procedures to handle reports about Internet intermediaries hosting illegal, infringing or undesirable content – are in widespread use. They provide a safe harbour if intermediaries remove content when receiving notification of *e.g.* a privacy breach or copyright infringement. Some participants expressed concern about over-notification by private complainants and lack of judicial review.

Notice and response schemes – whereby Internet intermediaries set-up procedures to handle reports about specific end-user activities – were also discussed. In the security arena, schemes are being implemented in some countries for ISPs to notify subscribers that are infected by botnets. Some countries are also implementing schemes for ISPs to forward notices of allegedly infringing material being exchanged via peer-to-peer networks. Some participants raised particular concerns regarding approaches such as graduated response, highlighting issues as to effectiveness, proportionality, fairness of the cost distribution, the need for an adequate judicial review process and oversight, as well as impacts on citizens' privacy and freedom of expression. Others stressed that they offered an opportunity for consumer education and behaviour change, and that due process elements were included to enable Internet users to challenge allegations of infringement.

Technical measures can be used by intermediaries to restrict access to specific classes of content or to avoid facilitating certain types of transactions with certain parties. For example, some content protection solutions in use by content hosting platforms compare user-uploaded content with a database of copyright ownership information to detect the original copyright ownership, allowing the right holders to decide whether to block it, promote it or monetise it. Other technical blocking measures such as IP blocking, blocking at DNS level and URL blocking are commonly used to block access to Internet sites, for

example, filtering content for child pornography. It was stressed, however, that Internet filtering technologies are prone to over-blocking, potentially inhibiting freedom of speech, as well as under-blocking, raising questions about their effectiveness. In addition, pre-scanning content uploaded to online platforms is, in many cases, impossible.

Dispute resolution mechanisms and redress are being implemented in particular by transaction-enhancing platforms such as online marketplaces and by payment providers. They provide procedures for buyers and sellers to resolve disputes. For example, in the payment provider industry, methods to address chargeback are implemented, whereby an issuer of a payment card can transfer the financial liability to the payment card acquirer, to transfer back the monetary value of a particular transaction.

Finally, ***education and awareness building*** among users of Internet intermediary platforms is considered crucial in many areas. For example, education campaigns for users and industries have been implemented in Korea to facilitate the responsible use of the Internet. Participants stressed the difficulty of educating consumers on security, the importance of users understanding data collection processes, so as to achieve meaningful choices relative to their privacy, and more generally, the importance of transparency.

Articulating common international principles for Internet intermediary policy would be timely

Participants were cautiously optimistic that in some areas there has been enough experience and work around the topic of Internet intermediaries by policymakers, the private sector and civil society, to identify and discuss high-level policy principles for the future. Given the global nature of the Internet and the cross-border services that Internet intermediaries often provide, an international convergence of approaches for the development of policies involving Internet intermediaries was viewed as essential, to provide effective guidance to the business sector. The OECD was identified as being able to help the emergence of such principles and to support their diffusion.