Executive summary

The functions of Internet intermediaries

Internet intermediaries provide the Internet's basic infrastructure and platforms by enabling communication and transactions between third parties. They can be commercial or non-commercial in nature, and include Internet service providers (ISPs), hosting providers, search engines, e-commerce intermediaries, payment intermediaries and participative networked platforms. Their main functions are: *i)* to provide infrastructure; *ii)* to collect, organise and evaluate dispersed information; *iii)* to facilitate social communication and information exchange; *iv)* to aggregate supply and demand; *v)* to facilitate market processes; *vi)* to provide trust; and *vii)* to take account of the needs of both buyers/users and sellers/advertisers. Related public policy issues concern notably their roles, legal responsibilities and liability for the actions of users of their platforms.

A source of economic growth and innovation

Against a backdrop of a broadening base of users worldwide and rapid convergence to IP (Internet protocol) networks for voice, data and video, Internet intermediaries offer increasing social and economic benefits through information, e-commerce, communication/social networks, participative networks and web services. They contribute to economic growth through productivity gains, lower transaction costs and wider ICT-sector growth. They operate and largely maintain the Internet infrastructure that now underpins economic and social activity worldwide. They help ensure continuing investment in physical and logical infrastructure to meet the network capacity demands of new applications and an expanding user base.

Because Internet intermediaries' services create network externalities, they need a critical mass of users. They also often operate in two-sided markets as intermediary between different groups, such as users and advertisers or buyers and sellers; they adopt pricing and investment strategies designed to attract both sides and balance their interests. For example, online advertisers, which now represent over 10% of global advertising revenue, allow intermediary platforms to provide increasingly sophisticated content and services at no monetary cost to users. Other revenue models include subscription and paid "on-demand" service models, brokerage fees, donations, and community development models for content or software.

The pace of change of Internet services and their technical complexity make it difficult to achieve stable, established business practices. Moreover, the blurring of boundaries between national statistical classifications and the creation of new areas of activity not necessarily based on transactions make measurement challenging. Nonetheless, the available data indicate that these markets are a significant source of growth, innovation and competition.

For example, US census data show that identified Internet intermediaries represented at least 1.4% of GDP value added in 2008: ISPs, data processing and web hosting providers, and Internet search engines accounted for 0.6%; retail e-commerce intermediary platforms for 0.2%; and wholesale e-commerce intermediary platforms for 0.57%. In comparison, the broadcasting and telecommunications sector accounted for 2.5% of GDP value added and the publishing industries for 1%.

Internet intermediaries stimulate employment and entrepreneurship by lowering barriers to starting and operating small businesses and by creating opportunities for previously impossible "long-tail" economic transactions (sales of many items in small quantities). They enable creativity and collaboration among individuals and enterprises and generate innovation. They facilitate user empowerment and choice, along with improved purchasing power through downward pressure on prices. By establishing user trust, they enable individuality and self-expression and can help advance fundamental values such as freedom and democracy.

Legal issues regarding Internet intermediaries' activities

Legal issues may arise because of the distribution of content or the provision of services on the Internet. While the vast majority of activities are lawful, illegal activities raise questions of liability. A text, image, song or user-generated video might be defamatory, contain illegal images of child pornography, infringe a copyright or incite racial hatred.

To what extent should Internet intermediaries be responsible for content originated by third parties using their network or services? How far should responsibility remain solely with the original author, provider or party distributing unauthorised content? What are the consequences, if any, of that responsibility for online innovation and free speech? If intermediaries are deemed even partially responsible for user content, should they be required to remove it or even to prevent its presence? Alternately, if only the third-party user is held responsible, what are the implications for controlling the dissemination of undesirable content, for copyright protection, or for the viability of legitimate innovative business models? If Internet intermediaries have liability, what will the impact be on their business models and economic viability, given the extra costs implied? Finally, how would liability affect online innovation and the free flow of information in the Internet economy?

Internet intermediaries' success in developing innovative technologies, policies and practices to deal with such issues should be underscored. Most have explicit policies prohibiting illegal activities by those using their platforms. These are often supplemented by specific policies and procedures to respond to particular policy concerns through voluntary individual actions or implementation of codes of conduct. Critical questions include: When do Internet intermediaries have business incentives to respond voluntarily to policy concerns regarding illegal or harmful content in the absence of legal obligation? What positive or negative implications do such voluntary actions entail? What corporate models or industry codes have been successful?

Internet intermediaries' evolving responsibilities and their response

Since about 2000, most OECD countries' approaches to limitation of liability for intermediaries for illegal or actionable content or activity by third parties have been converging through regulations defining liability regimes for Internet access providers, hosts and, less consistently, other types of intermediaries, based on two broad concepts. Intermediaries are generally not responsible for third-party content distributed without modification by the intermediary or for transactions taking place through their platform without their knowledge or control, nor do they have a general monitoring and surveillance obligation. The United States first implemented such a system in Section 230 of the *Communications Act*. However, specific obligations condition liability in certain circumstances, such as identifying users, preserving traffic data in response to requests, removing ("taking down") content upon receipt of a valid notice, etc. Such "limited liability" or "safe harbour" was implemented in Europe in the E-Commerce Directive and in the United States in the *Digital Millennium Copyright Act* (for copyright-infringing material only). Such frameworks for limiting liability, which may include certain conditions and obligations, have been instrumental in the growth of Internet service providers, e-commerce and emerging user-generated content (UGC) platforms.

New issues have arisen, ongoing issues have increased in scale, and the scope and types of Internet intermediaries have continued to evolve, creating regulatory challenges and a large quantity of case law. In particular:

- The notions of intermediary and content provider are increasingly blurred, especially on participative networking sites, potentially raising more subjective questions about neutrality and financial gain from hosting or linking activities.
- New types of intermediaries or intermediaries whose role has increased (search engines, social networking sites) raise questions about the need for distinct safe harbours. These involve the different categories of intermediary activity (hosting, conduit, linking, etc.) and whether small and large intermediaries need different rules.
- Pressures and priorities differ in terms of responsibility for copyright, pornography, privacy, consumer protection or security, raising questions as to whether "one-size-fits-all" and horizontal regimes are workable or desirable.
- *Ex ante* filtering rather than *ex post* take-down is increasingly provided voluntarily by some intermediaries for some types of content/activity or promoted by intellectual property right holders and law enforcement agencies, raising questions about whether and how the law should intervene, the cost, and possibilities for automation.
- Assessing the costs and benefits of new policy proposals on public and user interests is critical. Safeguards should be provided to ensure respect for fundamental rights including freedom of expression, protection of property, privacy and due process.
- The importance of multi-stakeholder bodies and other communication forums has grown. Consultation with all interested stakeholders in developing policies can help form the multi-stakeholder partnerships necessary to address complex emerging Internet policy issues.

- The global distribution of and access to online content and services by multi-national operators make the global dimensions of liability rules increasingly relevant.

Market forces, informally encouraged by governments, can often help resolve issues, improve standards of operation, or advance particular principled ideas, without the need for legislative intervention. Legal frameworks that have been publicly debated, with multi-stakeholder input, can help set parameters for self- or co-regulatory initiatives, with government acting to facilitate public-private partnerships and encourage broad-based involvement. Self-regulation is most likely to be effective when: *i)* industry has a collective interest in solving issues; *ii)* industry is able to establish clear objectives for a self-regulatory scheme; *iii)* the likely solution matches legitimate consumer and citizen needs; and; *iv)* the schemes yield rules that are enforceable through contracts and private legal actions or government enforcement, or both.

Case studies: examples of Internet intermediaries' practices

The case studies in Part II examine the practices and legal responsibilities of Internet intermediaries in each policy area, highlighting policy and legal implications such as effectiveness, technical feasibility, costs of compliance, appropriateness and reasonableness, privacy, speech, and due process.

The **global free flow of information** case study (Chapter 5) looks into actions Internet intermediaries can take to minimise the human rights and privacy implications of operating in countries that use Internet intermediaries to help censor the Internet. The Global Network Initiative is a self-regulatory initiative requiring its members to conduct *ex ante* civil rights impact assessments and develop risk mitigation strategies which many consider best practice. At the government level, whole-of-government approaches are needed to advance free flow of information objectives.

The **security** case study (Chapter 6) examines Internet service providers' role in improving the security of users who may lack sufficient incentives or ability to improve it. Malware-compromised home computers and botnets (networks of compromised computers) raise serious security threats. Japan's and Korea's public-private partnerships involve voluntary industry codes of conduct and standard processes for notifying, communicating with and helping subscribers whose computers may be infected by malware, processes which are being emulated elsewhere. Such initiatives can minimise potential negative effects on smaller firms and competition.

The **child protection** case study (Chapter 7) investigates measures to help curtail material on sexual abuse of children. Intermediaries forbid such content through their terms of service and co-operate with law enforcement and private-sector organisations to deny access to and payment for it. Increased international co-operation is needed to detect and close down sites with such content. Filtering based on blacklists has become widespread although in some OECD countries, this raises policy and constitutional concerns. Mandatory filtering regimes should provide for due process, accountability and transparency.

The **Internet gambling** case study (Chapter 8) examines policy responses to the online availability of gambling services based in other jurisdictions. The US *Unlawful Internet Gambling Enforcement Act* requires payment intermediaries to control illegal Internet gambling. Payment intermediaries block Internet gambling transactions in some

jurisdictions but allow them in others. Enforcement by payment intermediaries significantly reduced the US gambling market but can excessively block legal gambling, owing to legal ambiguities that give payment intermediaries substantial unsupervised discretion.

The **copyright** case study (Chapter 9) examines steps Internet intermediaries take to respond to online copyright infringement through notice and take-down, notice and notice, and graduated response regimes. The problem is sizeable although quantitative information is limited. Some countermeasures appear quite effective. Private arrangements may be effective but may only affect the specific parties and may not result from a transparent, multi-stakeholder process. Issues include the costs and effectiveness of different regimes and the efficiency and equity of cost-sharing arrangements. Expedited adjudication processes for allegations of copyright infringement to facilitate prompt and cost-effective enforcement while preserving due process should be considered, as should the impact of piracy on new legitimate and innovative business models.

The **counterfeiting** case study (Chapter 10) examines steps taken by search engines, online marketplaces and social networks regarding the sale of counterfeit goods. Some Internet intermediaries respond voluntarily to complaints and take pro-active steps to control counterfeit sales. Some courts seem satisfied with the current notice and take-down practices, but many find that further measures are required. Some argue that additional international harmonisation would help prevent overlapping and conflicting requirements. Enforcement efforts should weigh the benefits from reducing counterfeiting against the costs of enforcement; voluntary negotiations among affected parties can help determine an equilibrium point.

The **consumer protection** case study (Chapter 11) examines the role of payment intermediaries in providing consumers with protection from online payment fraud and with dispute resolution and redress mechanisms for online purchases. Both policy makers and payment intermediaries have strong incentives to develop a robust online marketplace. Issues include consumer liability limitations that may vary with e-commerce payment mechanisms and jurisdictions, and ways to encourage further development of fraud prevention and dispute resolution.

Key findings from the OECD workshop

- Intermediaries are increasingly important and empower end-users.
- Limitations on their liability for the actions of users of their platforms have encouraged the growth of the Internet.
- Depending on the issues, intermediaries' incentives may or may not align with public policy goals and they may or may not be well positioned to detect and address illegal activity.
- Governments and interest groups increasingly seek to hold Internet intermediaries to duties of care. There is increasing pressure for intermediaries to *act* rather than just *react*.
- Legal ambiguities weaken private-sector confidence, highlighting the need for clarification and guiding principles.
- All stakeholders play a role. Governments should set the rules of the game and facilitate private-sector initiatives.

- Technical capacity alone is insufficient; the variety of intermediary activities calls for differentiation.
- Fair cost distribution and due process should be taken into account. Quantitative information on costs and efficiency is needed.
- The impact of policies on civil liberties should be assessed and safeguards established.