Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

08-Sep-2010

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

SUMMARY OF THE WORKSHOP ON "THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES"

Held on 16 June 2010, Paris, France

This document provides a summary of the proceedings of a workshop on Internet intermediaries held on 16 June 2010 in Paris.

Karine Perset, tel: +33 1 45 24 19 83; Email: karine.perset@oecd.org
Alejandro Mantecón Guillén; Tel: +33-1 45 24 96 42; e-mail: alejandro.manteconguillen@oecd.org

JT03287951

Contents

MAIN POINTS 3

WELCOMING REMARKS AND INTRODUCTION 7

INTRODUCTION TO THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES 8

BALANCING OVERARCHING GOALS OF CREATIVITY AND FREE FLOW OF INFORMATION WITH OTHER POLICY OBJECTIVES 10

THE ROLE OF INTERNET INTERMEDIARIES IN STRENGTHENING CYBERSECURITY 11

THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING PRIVACY 13

THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING INTELLECTUAL PROPERTY RIGHTS 15

THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING CONSUMER SECURITY 18

ASSESSMENT AND LESSONS LEARNED 19

MAIN POINTS

1. This document contains proceedings of the OECD workshop on "the role of Internet intermediaries in advancing public policy objectives", held in Paris on 16 June 2010. The event was supported by the Norwegian government and was part of the project on Internet intermediaries that the Committee for Information, computer and Communications Policy (ICCP) is conducting.

Intermediaries are increasingly important and empower end-users

2. 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

3. 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

4. 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

5. 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…

6. The unpredictability of some court decisions, (or not), imposing duties of care on intermediaries was felt to create considerable uncertainty among industry stakeholders.[1]

…highlighting the need for clarification and guiding principles

7. 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

8. 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

9. 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

10. 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

11. 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…

12. 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

13. 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

14. 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

15. 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

16. ***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.

17. ***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.

18. ***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.

19. ***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.

20. 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

21. 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.

WELCOMING REMARKS AND INTRODUCTION

22. **Karen Kornbluh**, United States' Ambassador to the OECD, gave the opening keynote to the workshop. She emphasised the importance of the Internet and its increasing influence in the global economy. She underlined that this state had been achieved as a result of key policy frameworks and strategies. She highlighted the increasing challenges for policy makers to maintain such 'hands-off' policies in a rapidly changing environment characterised by increasing data flows across borders, heightened censorship and privacy concerns.

23. Mrs. Kornbluh further noted that the OECD is ideally suited to discuss the role of Internet intermediaries because of its historic mandates and ongoing streams of work. Recalling that the OECD is the place where regulators come to share best practices and to develop agreements, guidelines and conventions, she mentioned the Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" the Seoul Declaration for the Future of the Internet Economy, the Guidelines for Consumer Protection in the Context of Electronic Commerce, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as well as ongoing work examining policies to incentivise investment in broadband.

24. Mrs. Kornbluh concluded her remarks by asking workshop participants to focus on: *i)* what types of data would be useful for an emerging consensus in this area; *ii)* the high-level principles or values that were key to ensure the Internet continues to thrive; and *iii)* the specific policy strategies that have done best in balancing these competing needs of openness, trust and limited costs, noting that, for example, the United States has traditionally espoused voluntary industry codes of conduct safeguarded by regulators.

25. **Dimitri Ypsilanti**, Head of the Information, Communications and Consumer Policy Division at the OECD, thanked Norway for its active support in organising the workshop with the OECD. He explained that the project on Internet intermediaries is a horizontal project that stems from the 2008 Seoul Declaration on the Future of the Internet Economy. He provided guidance to workshop participants on what was expected from them for the day.

26. **Karine Perset**, Internet policy analyst in the Information, Communications and Consumer Policy Division of the OECD, introduced the OECD project on Internet intermediaries. She said that the first phase of the project had discussed the economic and social role of Internet intermediaries, whereas the second phase of the project would focus on intermediaries and public policy issues. She pointed out that the workshop would feed into the OECD report for Phase II of the project. She presented the different sessions of the workshop and their goal, and concluded that the workshop would discuss a delicate balancing act between, on the one hand, continuing to protect intermediary functions that are socially, economically and politically important and, on the other hand, balancing this with other policy goals, such as protecting security, privacy, intellectual property or consumers.

INTRODUCTION TO THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES

27. **Susan Crawford**, Professor at the University of Michigan Law School and moderator of the session, introduced the first session and encouraged speakers to be as clear as possible in the description of the concept and roles of Internet intermediaries. She highlighted that in the United States a relative state of immunity for Internet intermediaries has been adopted, and has led to economic growth and to numerous opportunities for speech and citizen participation.

28. **Mark MacCarthy**, Professor at Georgetown University, defined an Internet intermediary as an entity that connects end users and enables them to engage in transactions. They include ISPs, social networks, online marketplaces etc. He described three different frameworks for considering the responsibility of Internet intermediaries for their users' actions: *i)* the 'Internet exceptionalist' framework, based on Section 230 of the Communications Decency Act and industry self-regulation and on legal immunity for intermediaries under notice and takedown regimes; *ii*) the 'bordered Internet' framework – whereby local jurisdictions extend local law to intermediaries in areas such as Internet gambling, copyright infringement or filtering for child pornography;[2] and *iii*) the 'internationalist' framework – which arises when conflicts on local jurisdiction are difficult to resolve or when it is advantageous to harmonise rules.

29. **Lilian Edwards**, Professor of Internet Law at the University of Sheffield, responded to a question by the session Chair on whether there are special requirements for search engines. She first emphasized the trend towards increased liability of user-generated content (UGC) sites, resulting from pressure from the intellectual property rights holders on the extent to which UGC sites are complicit. She then stressed the increasing pressure from States, mainly on ISPs, to guard public morality by filtering child pornography, hate speech, racist content etc. She argued that these pressures combined may represent a tipping point time towards more liability on Internet intermediaries.

30. Mrs. Edwards reminded the audience that search engines are given a particular status of immunity within the Digital Millennium Copyright Act, but not within the European e-Commerce Directive, and warned that this impedes the confidence of search engine companies.

31. **Mario Dal Co**, Councillor to the Minister for Public Administration and Innovation in Italy, described Italy's three levels of regulation: *i)* general law protecting citizens' rights; *ii)* telecommunication sector regulation, which protects telecommunication customers; and *iii)* regulation which protects the citizens' privacy and the usage of public and private data. Mr. Dal Co emphasised the complexity of this system and the need to maintain a flexible regulatory system capable of adapting to rapidly changing technologies. He warned that using only the first level of regulation, which refers to general law, would insert inflexibility and inhibit the development of markets. In his view there is a choice between specific, strict rules which may inhibit market innovation, or instead, high–level principles which require a dynamic interpretation of existing laws. Mr. Dal Co believes the second approach should be preferred and that the risk that the borderline between legal and illegal market practices will remain indefinite is not a valid objection. He thought technology would move the borderline in any case: it is therefore better to adapt to technology changes and interpret the incidence of these changes on citizens' individual rights. He concluded on the necessity of co–operation between public authorities, markets, and consumers through intensive cultural interchange.

32. **Jean Bergevin**, Head of Unit of Retail and Information Services in the Directorate General for the Internal Market and Services at the European Commission, commented that the European Commission, in the E-commerce Directive (ECD) of 2000 focused on three specific services which Internet intermediaries

provide and where limited liability applies: mere conduit, cashing, and hosting services. The limited liability on these intermediary services applies because they are automatic, intermediate and temporary (mere conduit and caching) or passive (hosting). The safe harbour offered is conditional on the provider acting to disable access to illegal information once having actual knowledge of the illegality of that information. Differing interpretation as to "actual knowledge" and the "passive" nature of the information transmission will be examined in a forthcoming evaluation of the Directive foreseen for early 2011. He stressed that gambling, the only online service excluded from the ECD and therefore without safe harbour, has created an enormous amount of varying jurisprudence coming through the European Court of Justice due to the very fact that the conditional liability regime does not apply and that, as a consequence, Member States in seeking to regulate this area have sought to do so in different ways, including measures aimed at blocking sites. He emphasised that in his view, the main challenge is to enforce the existing legal provisions properly and clarify legal terms, as opposed to modifying or expanding the law that had stood the test of time.

33. **Gianluca Sepe**, Senior Lawyer of the *Autorita Garante della Concorrenza e del Mercato* in Italy, highlighted the tension on legislative frameworks between qualified immunity of Internet intermediaries and an increasing willingness of courts to establish a duty of care for them, thereby increasing their accountability. He noted the effort made by Internet intermediaries to respect reasonable expectations of users, stressed the unpredictability of court decisions in this area, and stressed that the business sector needed more guidance. He concluded his remarks by saying that a convergence of approaches at an international level would help to promote innovation and facilitate cross-border services by intermediaries.

Panel discussion

34. **Susan Crawford** asked participants to address the subjects of data collection and the difference between speech-enhancing intermediaries and transaction-enhancing intermediaries. Mark MacCarthy highlighted the complexity of obtaining information related to the activities of Internet intermediaries. He suggested focusing the discussion on costs and benefits of specific measures already in place. Jean Bergevin pointed out that companies are wary of sharing data for fear of losing liability limitations. Lilian Edwards shared her experience on informally gathering data on the use of notice and take down in the United Kingdom, emphasising how difficult it was to obtain. She further noted that ISPs have no incentives to share this data, and suggested the possible need for public sector intervention. She noted, however, that some firms, such as Google, were making efforts to make data available.

35. Susan Crawford asked participants to discuss “one size fits all” approaches versus differential treatment for different intermediaries. Mark MacCarthy stressed the need in all cases to have in place a process of transparency, openness and accountability. Gianluca Sepe emphasised the need to differentiate *actions* from *reactions*: while Internet intermediaries generally have a duty to *react* promptly to requests from consumers or governments, there is an open question as to whether they also have a duty to *act* in some cases. Lilian Edwards mentioned that one size does not fit all in terms of types of liability, underlining the specificities of intellectual property right holders issues and the potentially prohibitive costs of pre-emptive filtering for small ISPs. She pointed out the complexity of classifying intermediaries into speech enhancing and transaction enhancing categories because some of them offer more than one service. She emphasised the importance of using economic analysis.

36. **Jean Bergevin** pointed out that given the international dimension of the Internet it would be important to seek to agree to a guideline approach at an international level in order to give providers better visibility/certainty as to what they should do. **Milton Mueller** added that, if Internet intermediaries were to have a role on behalf of governments to enforce laws, there should be general criteria to meet beforehand, in particular: transparency, accuracy, accountability, precision and fairness in the distribution of costs. He warned that an intermediary strategy may need to reconcile diverse and potentially conflicting policy objectives. Mark MacCarthy mentioned the costs involved in Internet intermediaries’ duty to enforce laws on behalf of governments, and noted the need to determine whether governments should cover them or whether they should be shared among different parties.

BALANCING OVERARCHING GOALS OF CREATIVITY AND FREE FLOW OF INFORMATION WITH OTHER POLICY OBJECTIVES

37. **Susan Morgan**, Executive Director of the Global Network Initiative (GNI) and moderator of the session, introduced the panel and speakers to the participants. She believes that imposing legal liabilities on Internet intermediaries will limit ICTs' opportunity for creating social, economic, and human rights benefits. She warned that these liabilities can create two effects: *i)* encourage intermediaries to restrict speech or engage in self-censorship; or *ii)* discourage intermediaries from allowing anonymous use of their services. She emphasized that innovation is driven not only by companies but also by users themselves. She added that governments seeking growth of these technologies have tended to limit civil and criminal liability where intermediaries have provided the means for others to make content available, rather than creating the content themselves. She commented that governments are concerned about the use of networks for illicit purposes and, in some cases, government policies oblige intermediaries to proactively monitor the information that they transmit. She concluded her remarks by adding that the GNI, a non-governmental organization, seeks to protect and advance freedom of expression and privacy in the ICT sector.

38. **Daniel Weitzner**, Associate Administrator, Office of Policy Analysis and Development, Commerce Department, National Telecommunications and Information Administration (NTIA), quoted Benjamin Franklin and made the analogy between current Internet intermediaries issues and the freedom given to the press industry in the 18th Century. He suggested that policy makers emulate one of the basic principles of the Internet's technical architecture: "be liberal in what you accept and conservative in what you send", with illustrations from the technology, business practices, and policy making sectors. He emphasised the importance of following this principle when structuring the role of Internet intermediaries, with a bias towards limiting liability but towards encouraging law enforcement, consumer protection, and the free exchange of ideas.

39. **Anton Battesti**, Internet Governance Advisor, *Ministère des Affaires Etrangères et Européennes*, France, commented about the France–Netherlands initiative for freedom of speech on the Internet. He stressed the importance of freedom of speech in a context of continued high growth of Internet users. He outlined the initiative, which aims to promote freedom of speech and regulate its abuses by: *i)* establishing codes of conduct for companies exporting filtering and monitoring technologies; *ii)* developing international mechanisms to monitor State commitments to freedom of speech; *iii)* assisting cyber-dissidents, and; *iv)* giving the Internet a legal status that reflects its universality. He noted the importance of using international fora and institutions and for multi-stakeholder approaches to freedom of speech on the Internet.

Panel discussion

40. **Joe Alhadeff**, Vice President for Global Public Policy and Chief Privacy Officer for Oracle and Chairman of the Business and Industry Advisory Committee (BIAC) to the OECD ICCP Committee, inquired about how codes of conduct for technology firms might work, and noted that it was important to consider that the Internet is run by entities and that national initiatives would have international consequences. Anton Battesti explained that companies can develop software and technologies that may help governments in repressive regimes to identify cyber-dissidents. In such cases, it is better to identify potential misuse of the technologies before-hand.

41. **Katarina de Brisis**, Deputy Director General, Ministry of Government Administration, Reform and Church Affairs, Norway, thanked the OECD for organising the workshop and for its work on Internet intermediaries. She stressed that trust and confidence are essential in realising the potential of value creation on the Internet. She mentioned that security controls must be built-in. She pointed out that many stakeholders are involved in keeping the Internet robust and secure, and that co-operation between these stakeholders, including Internet intermediaries, is crucial. She introduced the panel and speakers.

42. **Rohan Buettel**, Assistant Secretary Networks Regulation, Department of Broadband, Communications and the Digital Economy, Australia, said that Australia was aware of the role ISPs could play in helping to solve cybersecurity issues. He described the development of the Australian Internet Security Initiative (AISI), which notifies ISPs of their customers' malware-infected computers. The Australian ISP cyber security code of practice is designed to generate consistency in cyber security messages and remedial practices between ISPs and their customers. He listed the four elements of this code: *i)* a notification management system for compromised computers; *ii)* a standardised information resource for end-users; *iii)* a comprehensive resource for ISPs to access the latest threat information; and *iv)* a reporting mechanism (back to a computer emergency response team (CERT)) in cases of extreme threat.

43. **Sven Karge**, Head of Content Department, Association of the German Internet Industry, warned that the high infection rate of end users in Germany threatens the economy and assists organized crime. He highlighted the Japanese cyber-clean centre initiative and the positive results it had produced. He presented the project of a central botnet disinfection centre, in close co-operation with the Federal Agency for Security of the Internet in Germany. He added that this project is an example of public private partnership, given that the Federal Agency for Security of the Internet is not only funding the project, but also contributing to its set-up phase.

44. **Bruce Schneier**, Chief Security Technology Officer, BT Counterpane, believes that, although Internet intermediaries have the ability to take on many actions to advance public policy objectives, they should pursue only a small number of activities involving their users/customers. He warned that there were security risks inherent to imposing policy objectives on Internet intermediaries, because intermediaries would have to build surveillance and control systems that would invite abuse by hackers, insiders, or simple function creep. Therefore, he said, policy makers should limit to the minimum possible the number of issues intermediaries are involved in.

45. **Ari Schwartz**, Vice President and Chief Operating Officer, Centre for Democracy and Technology, pointed to the rapid growth of third party applications for Internet intermediary platforms, and stressed the associated security and privacy risks. He noted that intermediary best practice included having procedures in place to take consumers complaints and try to solve problems quickly, reporting application developers to enforcement agencies, and not necessarily providing third-party applications with access to personal data. He stressed his belief that governments should focus on the application developers that are directly breaking the law, rather than intermediary platforms, and that they should encourage companies to offer tools to consumers to protect themselves.

46. **Cornelia Kutterer**, Senior Policy Counsel, Microsoft, stressed that all Internet stakeholders share a collective responsibility to make the Internet more reliable and trustworthy. She emphasised that integrated security processes in software development and co–operation and dialogue between all stakeholders are crucial to improve the security of users. She described the privacy process employed by Microsoft, incorporating privacy by default, design, and deployment in their products and services. She pointed out the steps taken by Microsoft to integrate privacy into their work with governments when responding to requests

for use of data. She finally emphasised Microsoft believes law enforcement co-operation and co-operation with governments is a key part of their responsibility to make the online world more secure.

Panel discussion

47. **Katarina de Brisis** highlighted the numerous approaches that can be taken by governments and industrial stakeholders, mentioning self-regulation, best practices and codes of conduct, co-regulation and co-operation. She further noted the Internet intermediaries' part of the collective responsibility to secure the Internet.

48. Katarina de Brisis asked the panel about the *kinds of incentives* governments may provide to get intermediaries to pursue best practices and responsible codes of conduct in the field of Internet security. Bruce Schneier noted that economic incentives may be adequate to drive Internet intermediaries to pursue best practices. Sven Karge doubted the need for incentives and pointed out the importance of governments establishing good relationships with industry stakeholders, to achieve jointly developed solutions. Ari Schwartz emphasized the industry stakeholders' need for clarity and the importance of having best practices that were defined and agreed upon by all parties. Cornelia Kutterer mentioned that incentives are already in the marketplace, for companies such as Microsoft. She mentioned the ongoing efforts in standardizing processes to make software more secure and doubted the need for more incentives at this stage. Mark MacCarthy wondered whether there were misaligned financial incentives in the ISP market, where ISPs may not want to forward information to their customers about security issues for fear of becoming liable.

49. **Jean Bergevin** pointed out the possibility of applying *disincentive* methods (*e.g.* "naming and shaming") to obtain a trustworthy product from design to delivery. He also mentioned that if ISPs risk losing market share due to their inability to empower users to take informed decisions, this is a powerful market incentive to empower users. Ari Schwartz mentioned that a desirable consequence of the naming and shaming practice is anti-virus vendors all finding out the same information and making adequate decisions on what to tell users and what default to set in their products. He mentioned that the reputation of a company on the third party applications market plays a role, and noted that reputation has a high impact in the advertising partner space. Bruce Schneier warned the naming and shaming practice works only in the exception, and if it becomes commonplace, consumers will not give it the necessary importance.

50. **Katarina de Brisis** questioned participants on the facilitation role of governments, to help intermediaries co–operate and agree on codes of conduct. Sven Karge emphasised the relevance of government support in regards to the regulatory landscape surrounding privacy infringement and data protection. For example, the press coverage of Germany's anti-botnet initiative was quite negative with erroneous interpretations by the media. He pointed out the need for governments to help create an understanding of the balance between privacy rights and the need to be in conformity with telecom law. Rohan Buettel commented that the Australian government opted to allow ISPs to decide the best way of dealing with this issue within their own business models. They must undertake one activity from a range of options in case a compromised computer is detected. Among other options, ISPs can contact the customer directly, prompt the customer to call a helpdesk, or temporarily quarantine the customer service.

51. **Daniel Weitzner** believes it is commendable for ISPs to invest resources in user education. He invited participants to think about a long-term process by which the right market signals could be delivered to those in the position to remedy the security problems. Bruce Schneier highlighted the difficulty of educating users. He mentioned that we currently have systems where the entity that is capable of mitigating risks doesn't have the incentive to do so, whereas the entity that does have the incentive is often incapable of doing so. He emphasised that policies should focus on changing the field on which the market operates by varying incentives, being very careful of unintended consequences. Sven Karge noted that the end users are the weakest part of the value chain, and suggested to improve their awareness and incentivise them to protect their own equipment.

52. **Katarina de Brisis** noted that ISPs are dependent on each other for finding solutions. In Norway for example ISPs have come to an agreement to fight spam. However, Bruce Schneier believes one benefit of regulation is that it limits free-riding among actors, and this may be difficult to achieve in negotiations between companies. Cornelia Kutterer stressed the importance of giving companies the necessary tools to fight cybercrime (*e.g.* the Cybercrime Treaty of the Council of Europe).

53. **David Banisar**, representing CSISAC, stressed the importance of involving users and issues regarding privacy, transparency and freedom of expression in public policy decisions. Ari Schwartz emphasised the reasons for supporting and encouraging self-regulatory frameworks to involve stakeholders in the decision-making process. Daniel Weitzner warned that ensuring transparency and due process is time consuming and not necessarily in companies' budgets. He suggested that in some cases governments should step in to help provide financial and institutional resources to support private sector efforts. He mentioned the importance of knowing at what time scale results could be expected from the Australian and German initiatives commented during the panel, in order to learn from these efforts.

THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING PRIVACY

54. **Hugh Stevenson**, Deputy Director of the Office of International Affairs, US Federal Trade Commission, and moderator of the session, introduced the panel, to focus on search-engines and participative networking platforms. He noted that approaches taken towards the topic might vary between jurisdictions because of different underlying laws (*e.g.* data protection legislation).

55. **Peter Fleischer**, Global Privacy Counsel, Google, described the case involving Google Italy and a video hosted on its site, because of which three employees, including Mr. Fleischer, were found guilty of privacy infringement. He explained that in Italy, it is not possible to conduct a criminal prosecution against a corporate entity, but only against a physical person. He described how a group of teenagers had uploaded a video that humiliated their disabled classmate onto Google's video site. He further noted that Google took the video off the site within two and a half hours of receiving notification. Mr. Fleischer explained that the E-Commerce Directive and its limitations on intermediary liability exclude privacy issues, creating legal ambiguity in Europe on what Internet intermediaries' responsibilities and potential liabilities are. He added that privacy resides on the concept of consent and that it is impossible for Internet platforms to discern whether a person has or not consented to the material related to him/her being on the platform. He stressed that pre-screening content is not only a controversial form of censorship, but also not feasible from a technical perspective. Finally Mr. Fleischer mentioned the launch by Google of an interactive map of countries around the world showing the number of requests from governments to obtain user data and to remove content.

56. **Gary Davis**, Deputy Data Protection Commissioner, Director of investigations, Ireland, mentioned that, from a regulator's perspective, Internet intermediaries are responsible for the protection of the personal data of their users. He added that users also share part of the responsibility, and emphasised the need to educate users despite the complexity of the environment. He highlighted the complication for Internet intermediaries in discerning personal data from non-personal data. He reminded the audience that many services offered by intermediaries are free, but that they use personal data to finance the provision of these services on two-sided markets. He pointed out that the challenge is to identify how much personal data is too much. He believes the policy response in these areas, where there is an ever-greater collection of personal data, is to either suggest greater regulatory oversight or industry codes of practice. He concluded his remarks

by making the case for enhanced co-operation between industry, policy makers, and regulators to ensure that the use of personal data is fair, as well as to provide more consistency to industry across jurisdictions.

57. **Yong Wan Ju**, Vice President of KISA (Korea Internet and Security Agency), stated that Internet users also share a responsibility to protect private data. He mentioned that governments should consider legal initiatives as a last resort, and should provide minimal regulation. He further noted governments should focus on education campaigns for users and industry to help protect personal data, and highlighted Korea's government efforts in this area. Mr. Yong Wan Ju introduced the i-Pin, a personal identification number for use on the Internet in Korea. The i-Pin is meant to act as a substitute for the social security number, given that the later includes personal information of its user, such as date of birth and gender.

58. **Anna Fielder**, CSISAC steering committee member/Privacy International Board of Directors, mentioned that 65 countries have data protection legislation, and many guidelines on privacy exist. She highlighted the fundamental conflict of interest that intermediaries have in protecting personal information, because their business models rely on monetising this same personal information. She added that, as a result, intermediaries manipulate 'user consent' or 'user control' through default settings, information asymmetry, and obscure privacy notices. She concluded that the challenge is to enforce existing legislation in a meaningful way: for example through the development of user interfaces that ensure people understand and give meaningful consent to the use of their personal information.

Panel discussion

59. **Isabella Maria Palombini**, from the Communications Department of the Ministry of Economic Development in Italy, highlighted inter-ministerial discussions on developing a code of conduct for Internet operators. She stressed that, in the absence of *ex-ante* control, operators should define the rules they will follow, and that a distinction mark would certify the operators that follow this code of conduct, to help users make informed decisions. Peter Fleischer referred to Google's Ads Preference Manager, which informs users about the preferences associated with their browser and gives them the opportunity to manage the categories of advertisement they would prefer to find.

60. **Bruce Schneier** presented a taxonomy of user data, using social networking sites as an example, differentiating: *i)* service data, which is provided to open an account; *ii)* disclosed data, which is entered voluntarily by the user; *iii)* entrusted data, taking as an example the comments made on other people's entries; *iv)* incidental data, which is about a specific user, but uploaded by someone else; *v)* behavioural data, which contains information about the actions users are undertaking when using the site and may be used for targeted advertising; and *vi)* inferred data, which is information deduced from someone's profile or activities. He underlined the importance of considering the different types of data in public policy discussions. **Yoshiaki Tojo** stressed the importance of differentiating two types of use of personal data: use of single records or use of data as part of statistical reference models. Referring to the notion of dynamic consent, he stressed the difficulty of withdrawing previous privacy consent made by users, and of ensuring the destruction of data. He pointed out that large players such as search-engines should work on detaching personally identifiable data from other data. Anna Fielder agreed with remarks about the complexity of data, and noted that it is possible to manipulate the consent of users making the default settings public rather than private.

61. **Michael Busch**, from the Directorate for Information Society and Media of the European Commission, described the Safer Social Networks Principles agreed upon by the European Commission and by 20 major social networking sites for the protection of children's private data. He explained that, as a result of the agreement, social networking sites must have an age verification system, children's profiles should not be searchable, default settings for all children's profiles should be private, children must have full control of the content, and all the features should be clear and easy to understand and to manage for them. **Hugh Stevenson** commented that the US Federal Trade Commission is also examining the issues in connection with the Children Online Privacy Protection Act (COPPA). Anna Fielder noted that the EC

agreement could be useful for the protection of adults private data as well. Peter Fleischer highlighted the privacy implications of verifying age on Internet platforms. He noted the need for some kind of identification or credit card number to confirm a person's age. He pointed out that this practice turns anonymous systems into identified systems, with serious implications. Gary Davis confirmed that there was not a satisfactory solution for age verification of children and adults. Cornelia Kutterer highlighted cultural differences in the context of public policies related to child protection, noting that laws vary regarding to the age at which a child can give consent and explaining that the identification process need not intrude on privacy if a claim-based system is set-up.

62. **Ari Schwartz** stated that third parties should be responsible for the information that they use, and reminded the audience that the question under discussion is rather whether Internet intermediaries should be responsible for the bad practices of another party, which is the one actually violating the law.

63. **Mario Dal** Co referred to **Peter Fleischer's** remarks, and added that in Italy there is a strong distinction between the judicial and executive branches, and emphasised the ongoing discussions seeking to improve the judicial system's efficiency, highlighting that Italy is a democratic country. He also stated that in his view, a company's right to make money should not prevail on a person's dignity. Daniel Weitzner referred to the Google Italy case, mentioning that it is precisely because of the complex privacy questions faced globally that questions of data protection and other individual rights are treated as matters of national concern and are handled as exceptions. He stated that these exceptions raise very important questions for intermediary liability that should be addressed. **Gabriel Dayre** from the Directorate-General for Health and Consumers of the European Commission inquired about the Italian teenagers who posted the offending content in Google's video site, and asked if they were warned of the implications of what they were doing beforehand. Peter Fleischer explained that in the Google Italy case, the teenagers were in the same classroom as their teacher while the video was being recorded. He added that prosecution of the teacher was going on separately, and noted that the teenagers were identified with Google's help and were sentenced to community service. He believes that there is clear notice of the terms of agreement a user must concur with when uploading a video in Google's site, and agreed that more education of the user community would be appropriate.

THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING INTELLECTUAL PROPERTY RIGHTS

64. **Mark MacCarthy**, Professor, Georgetown University, and session moderator, provided an overview of the different mechanisms that involve using Internet intermediaries helping to combat copyright-infringing material. He first mentioned the notice and take-down (NTD) mechanism included in the 1998 Digital Millennium Copyright Act. He described notice-forwarding procedures where intermediaries receive complaints of copyright infringement and forward them to their subscribers. He also mentioned graduated response mechanisms, which have not been in place for enough time to assess their results as well as other proposals to conduct URL-blocking and deep packet inspection (DPI).

65. **Trevor Albery**, Vice President of Anti-Piracy Operations, Warner Bros. Entertainment Europe, stated his belief that the over-riding goal is to achieve a safe and responsible Internet, with protection of intellectual property rights (IPRs) just one strand of that. He mentioned that policy solutions vary between the different types of intermediaries and between countries. He pointed out that voluntary arrangements between different stakeholders on this topic are the preferable route.

66. **Mita Mitra**, Manager, Internet & New Media Regulation of British Telecom, introduced new legislation in the United Kingdom, which deals mainly with ISPs and peer-to-peer illegal downloading. She noted that part of the legislation enables the State to introduce broader measures, such as web blocking. She explained that ISPs will keep lists of users for whom notices have been received and, at some point (yet to be

determined), right holders can request these lists which will enable them to pinpoint infringers through a unique identifier and not through personal data. She warned that the legislation does not address the issue of who the individual infringer is, but rather targets the subscriber.

67. **Gwen Hinze**, International Director, Electronic Frontier Foundation, stated that limitations on liability for copyright infringement for Internet intermediaries are necessary both for investment and innovation in Internet technologies and also for the protection of citizens' fundamental expression rights and privacy. She warned that without limitations on liability, Internet intermediaries would be forced to review all content passing through their networks and to restrict the ability of users to upload content to their platforms, for fear of liability. She stressed that, if liability is imposed on Internet intermediaries, legal and policy frameworks have to incorporate transparency, fairness, due process, proportionality and accountability. She added that network-level filtering by ISPs for potential copyright infringing material is ineffective because it can be defeated by encryption. She pointed out that graduated response regimes that require Internet intermediaries to automatically terminate user accounts on an accusation of copyright infringement, raise concerns about lack of proportionality and due process, particularly if done without judicial review.

68. **Yoshiaki Tojo**, Director, Information Services Industry Division, METI, Japan, introduced Japan's current legal framework on ISP liability and responsibility. He noted that Japan adopted the notice and take-down regime in its ISP Liability Act. He pointed out that ISPs make the initial judgement as to whether the claim is valid or not. Therefore the decision to take down was not as automated as in the United States' DMCA. He also pointed out the ambiguous treatment of link sites and search engines. Mr. Tojo believes it is important to examine the nature of the offense in the notice and take-down regime, differentiating treatment of commercial versus non-commercial offender and of repeat versus casual offenders. He also emphasised the importance of voluntary collaboration between right holders and ISPs with responsibility first for prime offenders, then platforms and finally, ISPs.

69. **Torgeir Waterhouse**, Project Manager, ICT-Norway, believes that online music stores such as iTunes showed that stores sometimes were not able to meet consumer expectations because of supply issues in the rightholder value chain back to the artists. He stated his belief that the solution to copyright infringement was not liability on ISPs, but rather making legal alternatives more attractive. He stressed that several Norwegian cases against the online music store iTunes showed that the store was not able to meet consumer expectations because of demands by right holders.

Panel discussion

70. **Milton Mueller** mentioned that copyright and trademark stakeholders failed to retain the control they had on their products in the traditional media world, where there were a small number of bottleneck distribution points. He added that having realised how expensive it was to translate these forms of control to the Internet, these stakeholders have shifted their attention to Internet intermediaries in the past years. He noted that indirect liability can reduce overall social cost when two conditions are met: *i)* the intermediary is in the best position to detect the direct party's bad action; and *ii)* the intermediary can internalise the significant externality associated with its activities. He pointed out that none of these conditions seem to hold in copyright enforcement issues (although they often do in the security realm). He pointed out that for IPR, involvement of intermediaries did not entail cost savings in terms of detection, that the value of copyright works would not increase because of more ISP responsibility and that any cost savings in enforcement would occur at the expense of due process. He also stressed that technical measures can only show that an automatically identifiable file has moved across the network, not specifying if a particular user is infringing or not.

71. **Antoine Aubert** from Google, stated that intellectual property enforcement is not a negative issue, and noted that the goal is to create an environment that can foster creation and lawful ways to best value this creativity. He commented that growth in the content distribution sector will come only as a consequence of new business models that emerge from the Internet and allow best monetising and valuing available content. He underlined the need to avoid intellectual property enforcement jeopardizing the development of the Internet. Yoshiaki Tojo believes there are additional aspects on which ISPs can co–operate with right holders to address intellectual property infringement issues. He suggested finding creative ways to reduce costs from product lines, to allow ISPs and copyright holders to cover some part of the economic losses they may be subject to when implementing mechanisms to protect intellectual property rights. Torgeir Waterhouse pointed out the high stakes due to the losses being incurred by copyright holders, but highlighted the need to avoid just shifting these losses elsewhere in the value chain and to avoid creating obstacles to innovation. He noted the importance of voluntary agreements and solutions.

72. **Christoph Beat Graber**, from the University of Lucerne, reminded the audience that in legal doctrine constitutional rights protect individuals against interventions coming from the state. He noted that on the Internet it is common to find confrontations where free speech infringements do not primarily stem from state but often from private activities. He referred to the results of a survey demonstrating a shift from primary responsibility towards secondary responsibility of Internet intermediaries. He warned that this shift is problematic from a free speech perspective because intermediaries are private actors and are not under constitutional scrutiny. He further noted that copyright enforcement may result in too broad protection of intellectual property rights and exceptions could not be assured because of the lack of flexibility of surveillance technologies.

73. **Gary Davis** referred to the remarks about the graduated response system in Ireland, explaining that it came out as a proposed method when the music industry took the largest ISP to court to require it to block and disconnect users who access illegal content. After engaging on some significant data protection issues, the music industry went back to court and sought a judgement from the high court as to whether there were actual data protection issues. He noted that the second largest ISP in Ireland will be before the high court challenging the same deal on the basis of the mere conduit principle.

74. **Trevor Albery** mentioned that graduated response type systems are an opportunity to educate consumers about illegal activity that may occur from their account and give them the opportunity to change behaviour. He stated that the system in the United Kingdom will give users an opportunity to challenge the allegation of infringement. He does not believe that implementation and operation costs of a graduated response system will be too high for this regime to function adequately.

75. **Mita Mitra** noted the imbalance of graduated response systems in terms of imposition of costs responsibility, both in terms of formal legal liability and in practical terms. She further noted that ISPs would have to engage in and fund new activities they would not otherwise have done, to the benefit of the copyright holders. She expressed her concern about the lack of a full impact assessment and analysis of market distortions between ISPs and between content providers and ISPs. **Gwen Hinze** agreed, stressing that the costs for Internet intermediaries in applying graduated response systems may have a negative impact on consumers. Mita Mitra warned that, in addition, the underlying issue of how much should rest on allegations of IPR holders needed to be addressed.

THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING CONSUMER SECURITY

76. **Graham Branton**, Deputy Director, Consumer and Competition Policy, Department for Business, Innovation and Skills, United Kingdom, introduced the session. He stated that making markets work requires consumer engagement, confidence and empowerment. He noted that lack of consumer confidence comes as a consequence of consumers not understanding security issues. Because consumers do not take into account security in their choices, security is not a driver of business decisions. He underlined the need to regulate at an international level when markets fail and the respective roles of regulation, education, and feedback systems.

77. **Stefan Krawczyk**, Senior Director and Counsel Government Relations Europe for eBay began his remarks stating that eBay is an e-commerce marketplace where the consumer-to-consumer auction model is becoming less significant. He emphasszed that eBay never owns the goods that are being traded. He explained that most users who have a negative experience on eBay never come back to the site and therefore eBay needs to make the online buying experience positive. He listed some of the measures taken to achieve this objective: *i)* making sure buyers use safe payment methods; *ii)* preventing fraudulent e-mails; *iii)* giving consumers a means to assess the trustworthiness of buyers; *iv)* fighting identity theft and other fraudulent activities; and *v)* educating and supporting users. He underlined eBay's co–operation with law enforcement units.

78. **Benoît Tabaka**, Legal Director, PriceMinister, stressed that consumer protection is essential to PriceMinister's objectives. He added that the company has three types of consumer protection responsibilities: *i)* towards the e-commerce industry; *ii)* towards third parties; and *iii)* towards users. He considers the feedback and reputation method to be potentially dangerous and not suitable for the protection of millions of users. He emphasised the need for the online marketplace industry to be proactive to detect harmful content, to prevent credit card fraud, and to develop consumer-oriented business models.

79. **Valentim Oliveira**, Chief Security Officer, SIBS – Forward Payment Solutions, Portugal, warned of the growing magnitude and sophistication of cyber-attacks. He stated that user education is a highly effective prevention method. He mentioned other security methods like CVV2, a three digit number at the back of the payment card, which has prevented a considerable amount of attacks. He pointed out Visa's 3D Secure has an added layer of security in which the consumer has to go through an authentication process before being able to perform payments. Mr. Oliveira highlighted some detection methods, noting that the card payment industry has made use of the installed base of fraud detection systems for traditional cards, adapting them to online payment.

80. **Peter Møller Jensen**, Vice President , EU Relations and Regulatory Affairs at the Legal Department of Visa Europe, pointed to the continued growth of e-commerce. He mentioned that developing tools for online authentication to further enhance consumer confidence and prevent fraud are key challenges in the payment space. He described the VBV (Verified by Visa) tool, which enables the financial institution that issues a Visa card to authenticate the cardholder during the virtual checkout process. He explained that the chargeback rules and procedures are a dispute resolution process set up between issuers and acquirers through contractual means and not a consumer right as such. Through the process the issuer of a payment card can transfer the liability for a transaction back to the acquirer of the transaction, who then has the right to further dispute it. Ultimately, Visa will solve the dispute if the issuer and the acquirer are not able to do so. Peter also questioned whether the current definition of Internet intermediaries is the correct one and whether it is too broad.

81. **Marzena Lipman**, Senior Policy Advocate at Consumer Focus stated that Internet intermediaries have evolved from invisible facilitators to market players that interact directly with consumers, not just facilitating e-commerce transactions but also influencing and determining access to and choice among online

services and goods. She pointed out that the growing reliance on intermediaries puts pressure on traditional models of consumer protection. She warned that online transactions are complex and the environment difficult for consumers to understand, but companies often fail to provide enough information about lines of responsibilities.

82. **Mrs. Lipman** spoke about redress mechanisms, stressing that from a consumer perspective, payment intermediaries fulfill a crucial role. She noted that placing redress obligations on payment intermediaries was seen as a clean and simple way to reverse payment in case of un-authorized use, non-delivery of products, or products that are faulty or not as described. She pointed out the lack of protection of non-credit card payments, such as debit card, pre-paid and mobile payments. She further noted that some credit card providers extend credit card protections to debit card holders, and added that this kind of measure is often not standardised but instead, is left to the discretion of the payment provider. She also mentioned that online dispute resolution mechanisms introduced by some online intermediaries are a welcome step forward to bridge consumer protection gaps. However this type of good practice needs to be adopted across industries, along with the extension of statutory consumer rights to redress in the case of digital content delivered electronically and consumer-to-consumer transactions.

ASSESSMENT AND LESSONS LEARNED

83. **Andrew Wyckoff**, Director, OECD Directorate for Science, Technology and Industry and moderator of the panel, introduced the session and encouraged all workshop participants to participate.

84. **Joe Alhadeff**, Vice President for Global Public Policy and Chief Privacy Officer for Oracle and Chairman of the Business and Industry Advisory Committee (BIAC) to the OECD ICCP Committee, stated that all stakeholders have an important role to play in combating illegal activity on the Internet. He noted that measures taken by Internet intermediaries to address illegal activity online must be consistent with applicable legal frameworks and must foster other legitimate public policy objectives. He pointed out that the complexity and taxonomy of information complicates the understanding of how to deal with the applicable laws.

85. Mr. Alhadeff concluded from the discussions that there is no unique solution for all types of intermediaries and policy issues, and that a one-size-fits-all approach could lead to unintended consequences. He stressed the need for additional information to better understand reasonable user expectations of free services that may be funded through the use of personal information. He suggested the OECD and governments consult with all interested stakeholders when developing policies in this area. He added that these policies should promote transparency, clarity of process, user education and outreach to facilitate the responsible use of the Internet.

86. **Eric Goldman**, Associate Professor of Law, Santa Clara University School of Law and representative of the Civil Society Information Society Advisory Council (CSISAC) to the OECD ICCP Committee, underlined the importance of the role played by Internet intermediaries, and mentioned that it is important to accurately define the concept "Internet intermediary" and to find common characteristics. He noted the differences between Internet intermediaries, such as different competitive entry barriers, types of competition and consumer relationships. Mr. Goldman pointed out the technical capacity of Internet intermediaries to prevent harm, but noted that the consequences of deputising intermediaries to exercise this

capacity on behalf of governments were not clear, that there may be implications for competition, and that it should not negatively impact due process.

87. **Roland Perry**, Representative of the Internet Technical Advisory Committee (ITAC) to the OECD ICCP Committee, warned that some measures may not be as effective as expected because of the characteristics of the Internet core infrastructure. He offered to contribute to the project with ITAC's advice and expertise where relevant.

88. **Susan Crawford**, Professor, University of Michigan Law School and chair of the session on "the introduction to the role of Internet intermediaries in advancing public policy objectives", mentioned the complexity of the topic, pointing out that Internet intermediaries are part of an ecosystem that includes users, application developers, platforms and ISPs among others, all playing different roles. She noted that other differentiations that may be drawn include those between expression enhancing intermediaries and transactional intermediaries. She explained that there are many values at stake in considering a potential role for Internet intermediaries in enhancing public policy objectives, and that these values, such as economic growth and freedom of expression are, in important ways, incommensurate. She concluded her remarks by stressing the importance for governments of enforcing existing law as well as of providing guidance for business on duties of care and of OECD work in the process.

89. **Susan Morgan**, Executive Director of the Global Network Initiative and chair of the session on "Balancing Overarching Goals of Creativity and Free Flow of Information, stated that the global nature, the complexity and the scale of the Internet generate unique challenges for balancing the free flow of information with other policy objectives. In her view, the desire for a robust and interoperable system, the creation of an open and vibrant Internet, and the belief that the free flow of information can not only facilitate innovation and economic growth but can also help advance the rights of freedom of expression and privacy have driven the Internet so far. Mrs. Morgan highlighted the changing legal landscape facing intermediaries and suggested the development of applicable policy principles, including fundamental human rights.

90. **Katarina de Brisis**, Deputy Director General, Ministry of Government Administration, Reform and Church Affairs, Norway, and chair of the session on "The role of Internet intermediaries in strengthening cybersecurity" highlighted the importance of governments and intermediaries interacting to increase security, although that role is fraught with risk. She stressed that governments have an encouraging and active role, should facilitate co-operation, discussions and development of voluntary codes, and should refrain from imposing regulations, relying on self and co-regulation where possible. She reminded the audience that security is a common goal of stakeholders.

91. **Mark MacCarthy**, Professor, Georgetown University, and chair of the session on "The role of Internet intermediaries in protecting intellectual property rights", noted that intellectual property was different from other public policy goals and that notice and take-down has been in place for a long time as has notice forwarding. He stressed that the challenge is to discern whether the current system needs to be expanded or updated. He highlighted the importance of business models in which content providers and intermediaries could collaborate. He added that his panel agreed on the importance of transparency and due process whereby the alleged infringer can have a say regarding the accusation but regretted the scarcity of information on private arrangements.

92. **Hugh Stevenson**, Deputy Director of the Office of International Affairs, US Federal Trade Commission, and moderator of the session on "The role of Internet intermediaries in protecting privacy", highlighted the need for clarity and understanding data collection processes from the user point of view, in order to achieve meaningful choices, for both children and adults. From the industry point of view, he highlighted concerns about the uncertainty of the obligations being imposed, and about imposing pro-active monitoring obligations. He emphasised the distress from the government side about private data collection and use and governments' interest in making education work and in considering legal initiatives as a last

resort. He mentioned some conceptual challenges that had been identified: *i)* distinguishing the obligations of social networks towards the users they are dealing with directly versus those whose information is acquired indirectly; *ii)* differences between intermediary liability and privacy law across jurisdictions; and *iii)* applying one policy to a whole taxonomy of data types or data collection processes.

93. **Graham Branton**, Deputy Director, Consumer and Competition Policy, Department for Business, Innovation and Skills, United Kingdom, and chair of the session on "The role of Internet intermediaries in protecting consumer security", said that where consumers are concerned, markets tend to develop platforms to meet consumer concerns about security and about payment systems. Regarding payment protection, Mr. Branton pointed out the considerable degree of consumer protection that this kind of intermediary offers. He warned that despite the consensus on not placing liabilities on Internet intermediaries, national laws are being used to impose duties of care, creating uncertainty as to what law actually applies in a given situation. He concluded his remarks by suggesting to address uncertainties through industry agreements, guidance and clarification of how existing laws apply to new scenarios.

94. **Andrew Wyckoff** pointed out that despite the economic crisis, the movement towards the Internet economy is accelerating, mentioning firms like Amazon and Apple, which have had historically record profits. He added that the success in this part of the economy may be partly because of the new regulatory embrace it took in the late 1990s, namely self and co-regulation but also due to safeguards by existing institutions and laws. He emphasised the need for more data regarding Internet intermediaries. He stressed the importance of articulating common values principles and due process type norms including transparency, accountability, redress, and proportionality. He recalled the point made that technical feasibility was not sufficient grounds for action and that policy makers needed to be aware of unintended consequences. He also stressed the importance of thinking through the economic/marketplace incentives and externalities and introducing market incentives and the important role of institutions like the OECD.

Panel discussion

95. **Susan Morgan** stressed the need to consider social development aspects, particularly human rights and democratic rights. **Stephanie Perrin**, on behalf of CSISAC, suggested the use of cost-benefit analysis or risk analysis to look at the impacts of contemplated actions. She warned that some liberties, growth opportunities and rights may be at risk, and that a mature analysis was needed because some of these may not be quantifiable.

96. **Mark MacCarthy** reiterated principles for assessing the success of work being done in this area: *i)* how well is the status quo doing? Do we need to make a change in the legal regime? *ii)* What are the costs and benefits of moving forward in this area? *iii)* What values are at stake? He highlighted the importance of taking into consideration the incentives for innovation, mentioning the case of payment providers and the innovation in taking the fraud liability off cardholders.

97. **Joe Alhadeff** noted that in some cases Internet intermediaries may not want to share data collected because they fear it might be used to assign additional responsibilities to them. He stated that data would not be standard across regions, intermediaries and operations, increasing the complexity of data comparison. He pointed out that case studies may help in getting information due to their context-sensitive nature. He warned that the rule related to credit cards does not necessarily incentivise healthier, responsible behaviour related to how a credit card is used. **Daniel Weitzner** suggested a focus on market analysis, quantitative and qualitative, of what intermediaries are doing. He stressed the importance of collecting relevant descriptive data for this topic. He noted that it had been possible to develop privacy guidelines because of sufficient experience with regulatory approaches, academic engagement and legislative approaches. He stated that he was cautiously optimistic that there has been enough experience and work around the topic of Internet intermediaries to reach a solution.

98. **Bruce Schneier** reminded participants that Internet intermediaries empower individuals by allowing them to publish, distribute and broadcast content. He warned that it is anti-empowering to turn intermediaries into law-enforcement institutions. **Katarina de Brisis** emphasised the social nature of human beings and noted that, if given empowering tools, they socialise. She warned that we may be trying to apply public policy objectives that belong to the past to future institutions of the digital economy.

99. **Achim Klabunde** of the European Commission (telecom regulation section) stressed the need to consider all the relevant public policy objectives, including connectivity and accessibility. He emphasised the need to identify the stakeholder that is best placed along the whole value chain to take on a role in advancing public policy objectives, and further noted that it may not necessarily be the intermediary. He pointed out that intermediaries should be entitled to compensation for any additional obligation they might receive.

100. Peter Møller Jensen mentioned that further work needed to be done on the definition for Internet intermediaries. He noted the differences between the payment card industry and other kinds of intermediaries, pointing out that in a payment transaction it is essential for some stakeholders to take on liability and emphasising the complex nature of each kind of Internet intermediary.

101. Gianluca Sepe pointed out that all the interactions discussed during the workshop relate to two-sided markets, and the problems that they pose tend to transcend the limits of single jurisdictions. He highlighted that the Internet's ability to generate benefits for all those involved depends ultimately on its capacity to include the participants, and further noted that regulatory fragmentation is particularly risky. He suggested the OECD act as a catalyst to help the emergence of best practices and to support the diffusion of these practices.

---

1 In addition, while in the United States search engines are provided a safe harbor in the Digital Millennium Copyright Act (DMCA), the lack of a particular status of immunity for search engines within the European e-Commerce Directive (ECD) is deemed to negatively affect the confidence of search engines in Europe.

2 The 'bordered Internet' is described by Jack Goldsmith and Tim Wu in "Who Controls the Internet: Illusions of a Borderless World," 2006.