Google contribution to the public consultation on the future of electronic commerce in the internal market and the implementation of the on electronic commerce (2000/31/EC)

INTRODUCTION:

Google very much welcomes the opportunity to contribute to this consultation on e-commerce and to suggest ways to foster the full potential of e-commerce in driving European growth and competitiveness. We believe that some of the issues addressed in this consultation have far-reaching implications for access to information, freedom of expression, participative democracy and cultural diversity online. It is therefore important that these topics should be given due consideration if Europe is to achieve its key objectives and realise its core values.

Benefits and perspectives for the development of e-commerce in Europe.

The Commission has made the opportunities of the digital age a key part of its EU2020 goals, not just in the Digital Agenda and competition policy, but as a key part of and contributor to the renewal of the Single Market project. E-commerce therefore has a critical role to play in meeting the European Union's key objectives, especially since it:

- enables more cross-border trade, with more competitive pricing and improved access to products and services for EU consumers and citizens
- gives businesses the ability to reach and engage with more consumers and is particularly helpful in unlocking previously unreachable markets for SMEs
- facilitates the establishment of new business models, offering increased convenience and lower prices in a wide variety of sectors (e.g. air transportation or banking)
- supports greater cultural diversity and distribution of cultural products across Europe, offering new opportunities for artists and the creative sector via new online content distribution platforms
- supports media pluralism and enables the development of services allowing European citizens to be better informed on and express their views in political debates at local, national and European levels

The benefits of enabling more commercial activity online are not limited to the online world either; they also extend to the off-line world. Online advertising is increasingly used by businesses to promote their activities at a local, national or European level, and there is clear evidence to show that this also drives offline purchasing behaviour and interaction with customers in shops, restaurants and offices across the European Union.

Over the years, Google has often been asked to quantify the broader economic impact of online business and e-commerce. In October 2010, we commissioned a study to better understand the nature and size of commercial activity on the Internet in the UK. The study, undertaken by the Boston Consulting Group, revealed that in 2009 the Internet contributed £100 billion to the UK economy. This is a contribution bigger than any other industry and, most significantly, the Internet economy is expected to grow by 10% per year. The full study can be downloaded here : http://www.connectedkingdom.co.uk/. Earlier this year, we also issued a report which conservatively estimates that in 2009, Google generated $54 billion of economic activity for American businesses, website publishers and non–profits. The report can be downloaded from the website: www.google.com/economicimpact.

In Europe, the value of the e-commerce market is estimated[1] to be between €100 and €150 billion a year. With an Internal Market of 495 million EU consumers, and the largest broadband market in the world (some 60% of European citizens are classed as "regular" Internet users) Europe ought to be a world leader in e-commerce. Yet today, European citizens lag behind in e-commerce terms: in 2009, 75% of US Internet users had bought a product online, as had 62% of Koreans - but only 54% of Europeans had done so, and there is significant variance in this figure across the member states. It is also important to underline the relationship between goods and services that are researched online but purchased offline. The Boston Consulting Group study estimated that in the UK in 2008 this figure was £ 40 billion, almost the size of the e-commerce market itself,[2] with so called "multi-channel buyers" often purchasing unplanned items in the offline marketplace that were researched online.

Google's role in the development of e-commerce in Europe.

Google's services contribute significantly to the development of e-commerce in Europe, providing businesses with platforms that enable them to reach global audiences easily.

- **Online search**: Google offers localised search results in more than 55 countries and in 132 interface languages.

> Every day, we see more than a billion searches for information, images, books and news, and over a 90 day period, at least 20% of queries are new. Search is often the starting point for Internet users looking for information about products they would like to buy, services they require or content they would like to access. A TNS study of 2008 found that 63% of Internet users had researched a product online before buying it in the past month. Web search is now also being "location-enabled", allowing users easy access to businesses offering the products and services they are looking for, in their local area, via Maps and mobile phones.

[1]Ref. p65 Europe's Digital Competitiveness Report (from DG DIGIT) - http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[2]The Connected Kingdom – How the Internet is transforming the U.K. economy - The Boston consulting 2010 : http://www.connectedkingdom.co.uk/

Online search generally aims to take Internet users as quickly as possible from the search engine to websites with content that is relevant and useful to them. Every click from a search engine to a website therefore offers commercial potential to the website owner or content producers. For example, each click from Google News to a newspaper or other publisher website is an opportunity for these publishers to value this traffic by showing ads, register users and win loyal readers. Google sends news publishers more than 4 billion clicks each month: 1 billion clicks from Google News and an additional 3 billion from services like web search and our personalised homepage service, iGoogle. This equates - on average - to 100,000 business opportunities for global publishers every minute of every day.

- Online advertising: Google offers a variety of advertising products online, through a model allowing international firms as well as SMEs to advertise their product and services:

AdWords presents consumers with advertisements that are relevant and useful for them, triggered by the query that is typed into the search engine. For businesses, and especially for SMEs, AdWords enables the promotion of products and services in a way that is financially accessible and highly measurable. AdWords is available in 41 languages and across 190 countries. In addition to these sponsored links, Google directs many potential customers to businesses for free via its search results. The economic value report of 2009 (www.google.com/economicimpact) conservatively estimated that for every $1 a business in the United States spends on AdWords, advertisers receive an average of $8 in profit through Google Search and AdWords.

AdSense offers websites ("publishers") the opportunity to maximise online advertising revenues by displaying ads supplied by Google on their own websites. The advertisements are tailored to the content of the site, and website owners can choose to have text, image and video advertisements displayed on their websites. The ads generate revenue that is shared with the website owner, who receives the majority of the revenue.[3]

Google AdSense generates billions of dollars of revenue for publishers and website owners every year. In each of 2008 and 2009, Google paid out more than $5.5 billion to its AdSense publisher partners, and in the second quarter of 2010 alone, Google paid out $2.06 billion to AdSense publisher partners. (See http://investor.google.com/financial/tables.html and look for the line item "Traffic Acquisition Costs" for further information.)

- Online content services: One of the key challenges for the future development of the Internet is to develop ways to monetise creative and cultural content. In recent years, Google has continued to innovate in this area, both technologically and through partnerships with content providers, to develop new and beneficial business models for content distribution.

[3]More information on revenues share for AdSense are available at: http://adsense.blogspot.com/2010/05/adsense-revenue-share.html

YouTube garners more than 2 billion global views every day and 24 hours of video content are uploaded to the site every minute. It is a user-driven community where people can express themselves by creating and sharing videos. YouTube is used by thousands of professional partners and major media companies around the world to make their content available online through branded channels, including hours of footage of cultural, political, news or sporting events.

It is also a responsible online platform with clear Community Guidelines that set out what is and is not acceptable, and clear policies for dealing with inappropriate videos and potential copyright infringing material. We make it easy for users to flag content they believe violates YouTube Terms and Conditions - and we remove any videos that do not comply.

To help video and music rights holders better manage their content on YouTube, we have developed the Content ID system, a unique rights management tool that gives rights owners the ability to determine for themselves how to manage their material on YouTube. After uploading a reference copy of their content, the Content ID system automatically detects matching material, and allows them to choose to:

- block user-uploaded videos;
- monetise their content by placing ads next to videos wherever they are uploaded; or
- track, i.e. acquire statistics about access and decide later what to do.

The majority of Content ID partners have preferred the monetisation option. 90% of all videos claimed through Video ID have created revenue for the owner, and over a third of YouTube's total monetised views come from Content ID. Content ID offers different solutions for those rights holders who want to keep benefiting from the wider dissemination opportunities of the web.

Through the YouTube Partner Programme, we enable content producers (large and small) to directly monetise their content as they upload it by displaying advertisements and sharing in the revenue. Many thousands of partners earn revenue in this way, and as at September 2010, the number of partners earning more than $1,000 per month through advertising is up 300% since the start of 2010. Some partners earn more than $100,000 per month through advertising. In total (as at September 2010) more than 2 billion video views per week are monetised in this way. This represents 50% year on year growth in monetisation of videos on YouTube.

Advertising on YouTube provides an effective way of remunerating artists and enabling the creative industries to generate revenue from the content that they make. It also means that content can continue to be created and uploaded, and that cultural diversity and heritage can be promoted on a European and international level.

In addition to advertising-based business models YouTube is also experimenting with paid for access business models and live streaming of events.

Google Books: Today, Google has successful partnerships with more than 30,000 publishers and authors worldwide. We are also about to launch paid access models for books, with an open, cloud-based platform for e-books. Google wants to develop a digital book ecosystem to be opened for everyone - publishers who are looking for additional ways to sell their books, retailers who want to expand into e-books but may not have the resources to do so, and readers who want to access their digital books from anywhere.

Google's future book services will enable consumers to preview books from participating publishers, and then to purchase those books from Google or one of our retail partners. The Google digital book will live on the consumer's online bookshelf and can be accessed from multiple devices -- whether it's a PC, a smartphone, a netbook, or a dedicated reading device.

- Open platforms and services: Google contributes to the development of open platforms and services supporting e-commerce.

Mobile devices are fast becoming the world's favourite way to access digital information. **The Android Platform** is a free, open source mobile platform that any handset manufacturer can use to create a mobile phone, and any developer can use to create and sell applications. Android was originally designed by Google and we continue to invest in the development of the platform, but it is a fully open source project managed and developed by the Open Handset Alliance, a grouping of more than 75 companies in the mobile industry.

As of September 2010, more than 200,000 new Android-powered phones are activated every day, and independent software developers have created more than 80,000 applications which are available for free and for sale via the Android Market - an online applications store. The Android marketplace is unique in that it supports open platforms, and allows any developer to post any application. Developers can distribute their applications via the marketplace after completing just three simple steps: register as a merchant, upload and describe their content and publish it. Ad developers can monetise their applications by selling them, but also through the ad-supported model which is enabled through Google mobile platform. The Android Market is available in 44 countries and is enabled for e-commerce (i.e. for application sales) in 32 of those countries.

Google Maps - over 80% of people look to search engines for their local information, more than any other source, and 20% of searches on Google.com are related to location. Google Maps allows users to search for information, such as specific businesses or services, and to view the results in their geographic context. Google Maps is a free, open platform that allows businesses to market themselves for free by creating their own profile within Google Maps via our Place Pages services. At present, there are 50 million Place Pages in Google Maps and local search. By claiming a listing in Google Places, business owners can ensure that potential

customers have access to the most accurate, up-to-date information available about their businesses.

Businesses can also use Google Maps technology - such as route descriptions, Street View and Google Earth Viewer - in their own websites, to make it easier for customers to visit them in person.

Finally, Google continues to experiment with new advertising formats in Google Maps and local search. We recently rolled out a new ads feature, called Tags, in the United States. Small businesses who have claimed a listing in Google Places can pay a flat fee of $25/month to enhance their listings when they appear on Google.com and Google Maps. This gives small business owners the opportunity to highlight the aspects of their business that they think are most important or unique to potential customers.

Google believes that this consultation on the e-commerce Directive is crucial to ensure that Europe achieves the full potential and economic benefits of the digital single market. If the current Directive has created the basis for e-commerce to emerge, it is vital to ensure that the European legal framework keeps supporting openness, consumer confidence and provides the level of incentive and legal certainty for new businesses and services.

ANSWERS TO SPECIFIC QUESTIONS:

I. Development and practice (Questions 2-31)

30. Do you consider that the offer of viewing sporting and cultural events on the Internet, for example by direct streaming, is sufficiently developed? If not, in your view, what are the obstacles to such development?

As pointed out in the introduction, YouTube is used by a great number of individual users, professional partners and media companies to make their content available online. YouTube has been a leader in developing a suite of tools empowering rights holders to fully manage their content and create new opportunities to value it online. YouTube has notably developed Content ID; a system allowing rights holders to produce unique identifiers of their copyright protected audiovisual works. If such works are then identified, then rights holders are empowered by being able to decide what should be done with this content, including by monetising it.

YouTube has adopted this approach in line with the e-commerce Directive and gone beyond the legal obligations applying to intermediaries in the context of this Directive, creating an environment offering new opportunities to value content and copyright online. Such innovative services, and collaboration between Internet intermediaries and rights holders, can only be developed under a legal framework providing for the legal security needed for intermediaries to innovate. As illustrated in the answer to Question 53, court decisions challenging intermediary liability do not only call into question the delicate balance needed to support users' creativity and freedom of expression, but negatively impact on the Internet's innovative and entrepreneurial spirit and in certain cases act as a barrier to trade.

As for the development of new services supporting online access to cultural events, Google considers that the key is to allow for greater transparency, a simplification of the collective licensing process and a reduction in some of the inefficiencies created by the existing licensing regime. The current landscape provides for significant transactional costs in terms of the number of licences required to operate in any given territory, which impedes the ability to monetise content and increases time to market. The current uncertainty following the various repertoire withdrawals (on both a rights-owner and society basis) and the consequent fragmentation of the licensing landscape has made things extremely complex.

As YouTube, we have sometimes been faced with contradictory assertions as to what it is that can be licensed under any particular agreement. Party A will tell us they can license global repertoire, then party B will tell us that their repertoire, or at least a portion of it, has been withdrawn from party A's mandate. This is often difficult to corroborate and frustrates the negotiation process. So, in short, the breadth of repertoire available to be licensed (or at least from whom it can be licensed) still remains cloudy.

As to the territorial scope of repertoire, we welcome multi-territorial licensing but believe that certain conditions need to be met. Local market conditions need to be reflected in the license fees charged for any particular country. Commercial users should also not be expected to double pay for rights cleared elsewhere or for rights they do not exploit.

On the practical side, and assuming a licence does not provide coverage for global repertoire, there needs to be disclosure by rights owners and societies of all relevant identifying data in a standardised format that can be utilised by the user. A global repertoire licence means repertoire information isn't required in advance. In the absence of a global repertoire licence, we need to know in advance where a particular rights owner's repertoire is incorporated so we can monetise, or not, the content where we know the relevant rights have been cleared.

Having a transparent and efficient licensing system benefits all concerned, not least the rights owners and creators of local repertoire: it encourages cultural diversity by swelling the volume of content available on services and broadening its scope of distribution, and it minimises the cost of administration, thus increasing the total share of revenue that can ultimately benefit to artists.[4]

II. Derogations from Article 3 (Questions 32-37)

36. In your view, does the purchase and sale of copyright protected works subject to territorial rights and the territorial distribution of goods protected by industrial property rights, encourage or impede cross-border trade in information society services?

[4]See Google contribution to the online commerce group "issues paper" - http://ec.europa.eu/competition/consultations/2008_online_commerce/index.html

The exclusion of IPR from the country of origin principle impedes cross-border trade in information society services. The application of territorial rights limits the reach of such services, and does not allow them to be widely available across the Digital Single Market. This is particularly true in the field of copyright where licensing from the different right owners needs in many instances to be acquired on a country per country basis. As pointed out in the answer to Q30, this calls for a simplification of the collective licensing process and a reduction in some of the inefficiencies created by the existing licensing regimes.

IV. Press on the Internet (Questions 50,51)

51. In your view, is it necessary to ensure more transparency on the origin of the contents presented by news aggregators of information(1)? If so, by which mean(s)?

Google's core business is search--we aim to quickly provide our users with an answer, or to put them in touch with the content they are looking for. Whether a user is looking for a website, a news story, an image or a blog post, Google search results clearly identify the source of information and take users to the source. Services such as Google Search or Google News are not only clearly identifying the source of the information, but are also also taking users who click on the links directly to the source. In fact, we send more than four billion clicks each month to news publishers via Google Search, Google News, and other products. That is, every minute we send approximately 100,000 visitors to news publishers around the world. Except when we licence content from news publishers, Google News does not host news publishers' content; instead, it shows a small amount of text to give an indication of the story's subject and its source, and then redirects users to full versions of the news content.

The goal of Google News has always been to offer users the ability to access varied perspectives on a story in order to help them better understand current events. To that end, Google indexes more than 50,000 sources in dozens of languages from around the world. The big news events of the day are identified and ranked by computer algorithms that reflect the publishing activity – the collective news judgment – of news organisations. Then individual articles are automatically selected and ranked based on factors such as freshness, location, relevance, and diversity of their content, without regard to political viewpoint or ideology. Google News shows only a headline and sometimes a "snippet" – just enough for someone to decide if they're interested in reading the story. For this snippet to be useful it must give enough information, including the original source, for users to choose which result to click on. Clicking on the link takes them directly to the publisher's website. They do so at a rate of about one billion times a month from Google News alone.

We therefore see services like Google News as presenting a business opportunity for news publishers, and a service for users, helping readers find the news they seek. It is worth noting that search engines themselves do not derive a significant amount of revenue from news content. Many search engines generate revenue from displaying simple text ads near organic search results; advertisers bid for that placement and pay only if someone clicks on the ad, making it a highly targeted, relevant, and measurable form of advertising. But the real money in search engine advertising is in highly commercial queries for goods and services in such areas as shopping, health, and travel. (For example, Google generates only a tiny fraction of its search revenue from queries that we categorise as News & Current

events; while searches for terms like “canon powershot digital camera” are very attractive to advertisers, news-related queries often trigger few or no ads at all.)

While Google believes that Internet search provides revenue opportunity for the news industry, we also believe that publishers are to be in control to best value their content online, and have the ability to decide whether their sites are indexed at all, what of their sites is indexed (if they choose to allow indexing), and whether and on what terms a consumer is permitted to access their sites (e.g., whether the content sits behind a pay wall of some sort or, at the other end of the spectrum, is freely available).

Publishers have simple tools at their disposal to communicate instructions about whether they want search engines to index their sites, and Google’s policy has always been to fully respect those instructions. For example, using what is called the Robots Exclusion Protocol (REP) (which is the de facto industry standard used throughout the Web for more than 15 years), a site administrator who wishes to remove her website from Google’s index can easily do so using a “robots.txt” file.

Through the use of the robots.txt file and the no index meta tag, website owners are able to prevent their sites – or specific content on their sites – from being indexed by Google’s crawler. In fact, website owners are even able to specifically prohibit Google from indexing their site while allowing other Web crawlers to do so. Thus, website owners may easily exclude content from the Google index. Meta tags also allow a much deeper level of granularity. For example, publishers can instruct Google or other search engines to index articles but not images or to display headlines but not snippets. As for news publishers they also have the faculty to exclude their all or part of their website from Google News, but keep it in Google Search.

Google provides other tools for news publishers. On the advertising side, Google’s AdSense platform helps publishers generate revenue from their content by providing relevant advertising and improving the connection between advertisers and consumers. In 2009 alone, Google shared more than $5 billion in revenue with AdSense partners. In addition, many major media companies, including online newspapers, use Google’s DoubleClick platforms to manage, and maximise the value of, their most valuable online advertising inventory – the display ads they sell directly – to ensure that the right ad is placed in front of the right consumer at the right time. Google has invested significantly in these products, launching the new DoubleClick Ad Exchange and the upgraded DoubleClick for Publishers platform in the past 12 months.

In close partnership with news publishers, Google is also developing new formats for displaying and consuming news – such as Fast Flip, Living Stories, and YouTube Direct – which aim to improve the user experience and, consequently, increase the amount of time people spend with news on the Web. In October 2010, Google also announced that it will grant $5 million to non-profit organisations to finance projects on innovation in digital journalism, all around the world. In these and other ways, Google has worked productively with many individual news organisations and the broader journalism community. Most of these news providers share the vision that the future lies in embracing consumer preferences and collaborating with Internet companies.

V. ISP Liability regime (Questions 52-69)

We are now truly witnessing the development of the information society: a society where information is not only consumed, but also increasingly produced and exchanged by citizens through blogs, social networks, video sharing, consumer reviews and transactional marketplaces, to mention but a few. Information society services have become a fundamental way in which citizens effectively exercise their freedom of expression or association, their political and social consciousness, their creativity and cultural diversity. This is all made possible as Internet users are allowed to access and share information on open and inexpensive (often free) platforms, without being subject to prior authorisation or review.

The rules on ISP liability limitations are at the core of such development: without them, no network or service enabling expression and access to information can be sustainable or socially acceptable. Making ISPs liable for any content accessed or made available through their services, would call on ISPs to systematically monitor this content. With the exponential growth of information being created and distributed online, such a monitoring is not only impossible, but also not socially desirable. How could any operator reasonably review and analyse the legality (under all applicable rules - copyright, trademark, privacy, defamation, unfair competition - and under all applicable national laws) of each and every comment left on a site, of each photo posted on a blog or each video shared on a platform (e.g. an estimated more than 24 hours of videos are uploaded on YouTube every single minute)? Who would accept that ISPs should substitute themselves for judges to decide on which content he/she could access or make available? Just as in the offline environment it is key for liability to lie with the person who is effectively accessing or making available illegal content, and not on intermediaries.

52. Overall, have you had any difficulties with the interpretation of the provisions on the liability of the intermediary service providers? If so, which?

In general, the provisions on ISP liability have been correctly understood and applied in many European jurisdictions and on many types of information society services. That said, inconsistent interpretations and implementations of ISP liability provisions across the Internal Market are raising a set of difficulties for ISPs, creating legal uncertainties hampering the development of their activities, and the achievement of a Digital Single Market:

1. Civil and criminal liabilities: There is a lack of clarity across all Member States that the provisions in Articles 12-14 apply to both civil and criminal liability. While some implementing legislation are clear on this (e.g. in the UK, Ireland and France), it is not expressly stated, and not clear at all in other countries, raising major illegal uncertainties for ISPs. There is a need for the Commission to reaffirm that ISP liability limitation applies to civil and criminal liabilities to provide the level of legal certainty needed for ISPs to operate across Europe.

2. Separated assessment of intermediary activities: Many Internet companies operate a variety of services and handle third party content in a multiplicity of ways. There is a need to

clearly separate activities when considering the limitations of liability in the Directive. Without uniform approach to this critical issue, there is considerable scope for disharmony and differences in interpretation.

To underline the point, Google considers the following decisions on this point to be both relevant and correct:

(a) The UK High Court's approach as decided in Kaschke (which was a defamation claim in relation to hosted content, Kaschke v Gray and Hilton [2010] EWHC 690 (QB), 29 March 2010, at paragraph 69):

> *"However in my judgment that is not determinative of the question raised on this aspect of the appeal because it still does not necessarily identify the information society service whose provision is referred to in [Article 14]. Is it the storage of the particular information provided by the particular recipient of the service the storage of which results in the liability which would exist but for the exemption conferred by [Article 14], or is it the storage of all the information which is provided by all recipients of the service?"*

After considering the legal arguments, the Court decided (at paragraph 75):

> *"...the question to be asked is whether the information society service provided by the defendant in respect of the information containing the defamatory words which would otherwise give rise to liability consists only of and is limited to storage of that information. If the answer to that question is that it does consist only of storage of the information, [Article 14] immunity is potentially available even if it would not be available in respect of other information also stored by the defendant in respect of which the service provided by the defendant goes beyond mere storage."*).

In other words, consider the specific information containing the allegedly illegal content and ask: "was the information society service provided in respect of that information limited to the storage of that information?" If "yes", then the hosting limitation of liability is potentially available to the information society service (subject to satisfying the extra conditions).

We submit that this approach provides the granularity and focus required for the limitation of liability provisions to work effectively with modern, rapidly evolving, Internet services.

(b) The Irish High Court's approach in Betfair: A gambling operator hosted a web forum (chat room). While gambling is excluded from the e-commerce Directive, the chat room activity was considered a separate activity and held by the Irish High Court to be an information society service and a hosting service under Article 14 (Mulvaney & Ors v The Sporting Exchange Ltd t/a Betfair [2009] IEHC 133, 18 March 2009, at paragraphs 4.8-4.16).

On both point 1 and 2 above, we agree firmly with the Commission's statements in its First Report 2003 (page 12, paragraph 4.6) and the Commission Proposal 1998 (page 27). Google believes that in light of the developing case law around Europe, and the rapid pace of technical development of Internet services, it would be important for the Commission to reaffirm that the Directive covers "liability, both civil and criminal, for all types of illegal

activities initiated by third parties" and that "The distinction as regards liability is not based on different categories of operators but on the specific types of activities undertaken by operators."

Accordingly, in assessing whether the limitations of liability in the Directive apply, the court should conduct a precise assessment of the service provider's activity in relation to the specific allegedly illegal content - as was done in Kaschke and Betfair - and not some broad, sweeping or overall assessment.

***3. Conditions required for ISP liability limitation to apply**:* There needs to be clarity that the conditions set out in each of Articles 12-14 are both necessary and sufficient in order for a service to be covered by the limitation. Varying interpretations and additional conditions and tests should not be introduced on a country by country basis. Otherwise, as noted in the Commission Proposal 1998 (page 12) divisions between Member States, issues of "forum shopping" will arise and there will be significant uncertainty for information society services in the EU.

The European case law surrounding video hosting platforms and copyright offers an interesting illustration of this point. After a number of varied decisions, French courts including the Court of Appeal confirmed that video hosting platforms (e.g. Dailymotion, YouTube) were hosting services under Article 14 - the latest decision being Magdane v Dailymotion, Paris Court of Appeal, October 2010. Likewise, in Spain, after initially granting an interim injunction for the claimant, the Madrid court held on the merits that YouTube was a hosting service under Article 14 Telecinco et al v YouTube LLC, Commercial Court of Madrid, Judgment No.289/2010, 20 September 2010.

In stark contrast, in August 2010 in Germany, the Hamburg court held that certain videos uploaded to YouTube by users should be treated as content appropriated and provided by YouTube itself and not covered by Article 14 (applying the German "zu eigen machen" doctrine, BGH decision I ZR 166/07 of 12 November 2009 (Chefkoch)) Peterson v Google Inc and others, Hamburg Regional Court, 308 O 27/09, 3 September 2010. In essence, the host limitation of liability was not available to YouTube because of way in which user generated content was presented and displayed. This is despite the fact that there is no reference to presentation or display in Article 14 or the German implementing legislation for it. The zu eigen machen doctrine is not embodied in the e-commerce Directive and has been applied in Germany to Internet services with a lack of consistency across court decisions.

In December 2009, the first instance court in Rome granted an interim injunction against YouTube to remove videos of a certain TV programme. It appears that the court took the view that YouTube was not covered by the hosting provision under Article 14. The reasoning was unclear and YouTube appealed. A few weeks later the Appeal Panel upheld the injunction, made no clear decision in relation to YouTube's status under Article 14, stated that it did not appear reasonable to find a total lack of liability for copyright infringement, confirmed that under Article 15 YouTube was under no general obligation to monitor and that RTI did not have to identify each allegedly infringing video because the modality of enforcement of the injunction was being addressed in separate proceedings (in brief, RTI would use YouTube's Content ID system) RTI and others v. YouTube and others, Appeal

Panel decision of Civil Court of Rome, IP Specialist section, 22 January 2010 and Court of Rome, Section IX, RG n.54218/08, 15 December 2009.

Each of the above proceedings (Telecinco, Peterson and RTI) continue.

Differences on national lines as described above upset the level playing field between Member States for information society services. They create a situation where despite the harmonising efforts of the legislation, in practice, certain countries have a more favourable environment for hosting services than others. The situation does not create the conditions for innovative services to develop in Europe.

All of this is in sharp contrast to the clear and pragmatic decision of the US court in Viacom/FAPL - it is worth recalling that the claimants in parallel proceedings included EU-based parties, for example, the English Football Association Premier League Ltd (Cases: Viacom et al v YouTube et al, 07 Civ. 2103 and The Football Association Premier League Ltd, et al v YouTube et al, 07 Civ. 3582, US District Court (S. District of New York), 23 June 2010).

4. Clarification is required that there is no liability on the intermediary where none exists under applicable law. The limitations on liability do not themselves add liability. These simplistic sounding sentences embody an extremely important principle. In other words, circumstances must be such that if it was not for the limitation of liability under the Directive, the service provider would have a liability for the information under applicable law. So, for example, this was dealt with by the UK legislator as follows (in Regulation 19 implementing Article 14):

> *"Where an information society service is provided which consists of the storage of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable...."*

The words in parenthesis clarify the point and it would be extremely helpful if that clarification was made EU-wide. To put it another way, where the intermediary is not liable (for whatever reason), then putting the intermediary on notice does not create a liability, unless applicable law provides otherwise. (By "applicable law" we mean applicable legislation, court decisions, etc). Only the legislators and the courts may decide whether an intermediary should be liable in particular circumstances. Some examples follow: (a) under applicable law, contrary to what the complainant or claimant claims, the intermediary may be neither liable as a direct tortfeasor nor under an accessory theory; (b) in relation to defamation it has been decided in the UK, that certain kinds of intermediaries are not publishers; (c) under IPR law, the validity of the claimant's rights may be challenged, or the intermediary may fall within a statutory exception, or exclusion, etc.

This clarification is needed because in our experience, huge numbers of complainants take completely the opposite approach. They argue along the line that liability is **imposed** on the intermediary upon notice of an **alleged** illegality and **because of** Articles 12-14. Trying to explain that this is not the way the limitations work is a massive burden that intermediaries have to discharge daily. The numbers are voluminous but such discussions do not often end up in reported case law.

5. Hyperlinks (including Embedding) and search engines: There is specific inconsistency in relation to hyperlinks and search engines, which are key for the functioning and access to information on the Internet. These are expressly included in some MS' implementing legislation but not in others. In addition they are not treated consistently by courts.

By way of illustration, in the UK case TVLinks (R v Rock and Overton, Crown Court, Gloucester, 6 February 2010), the mere conduit Article 12 provided a defence to alleged offences of criminal copyright infringement for a website providing links. In contrast, in relation to the Google News Search service, the Belgian court in Copiepresse stated that the ECD is "not relevant". In yet further contrast, in Thumbnails (I ZR 69/08 issued on 29 April 2010) the German Bundesgerichtshof considered that Article 14 should apply to Google's image search service.

When considering hyperlinking generally, it is important to also provide for embedding. The legal treatment of embedding is subject to much legal debate, for example:
- There have been a number of cases in France over news aggregators and embedded news tickers (where embedders have been considered re-publishers of defamatory information).
- Google Video: we have faced liability for embedding third party (infringing) videos in relation to this video search service.
- Some collecting societies argue that additional licenses and payments are required from every website that embeds music videos. That kind of model is just like claiming that every hyperlink to a site must be paid for by the site. Such an approach would halt the development of the information society in the EU.

For the future, we consider that search engines are best treated under provisions similar to mere conduit (Article 12). This is discussed further below (under Q63).

***6. Disturbing trends that chip away at the principle of no obligation to monitor*:** These include the idea of take down, stay down, which effectively introduces a forward looking monitoring obligation on the service provider; attempts to impose filtering on service providers; broad injunctions to prevent infringement that cannot be complied with and require blanket monitoring; and in Germany the doctrine of "disturber" or "interferer" liability (*Störerhaftung*). We will discuss below the importance of the no obligation to monitor principle (Article 15) and why these sorts of measures are unworkable and destructive to the information society.

7. The imperfection of putting the service provider in the position of a judge: Service providers are increasingly being forced into making determinations of illegality, when often those are complex legal judgments whose rightful place is in a court. How do we know if a blog is defamatory? How do we know if consent has or has not been obtained? How do we know if a trade mark is being used lawfully?

8. The need for a clear uniform approach to the meaning of "actual knowledge" and "expeditious". Ideally, given the nature of e-commerce, this would be global or if not, at least consistent across the EEA. We describe why actual knowledge is important, its

essential elements and what should not be considered actual knowledge. We explain why a flexible interpretation of expeditious is required.

***9. Voluntary measures by service providers to prevent illegal content on their service should be encouraged, not discouraged*.** How such measures fit into the limitation of liability regime needs to be thoroughly considered. Responsible service providers should not be penalised for engaging in such voluntary measures, for example, by loss of their limitation of liability.

***10. The technology neutral approach was correct and should be applauded. A flexible approach to the limitations of liability is required for the future*.** We provide some thoughts on both these matters.

***11. A standardised notice and take down regime would be hugely beneficial*.** We discuss the principles it should embody, the options and provide our thoughts on a workable system.

53. Have you had any difficulties with the interpretation of the term "actual knowledge" in Articles 13(1)(e) and 14(1)(a) with respect to the removal of problematic information? Are you aware of any situations where this criterion has proved counter-productive for providers voluntarily making efforts to detect illegal activities?

The notion of "actual knowledge" is a vital ingredient of the European regime and raises a set of difficulties. Identical words also appear in the US DMCA. In order to encourage a global level playing field, consistent interpretation of these words is highly desirable. In this regard we refer to the recent judgment of the US court in the Viacom/FAPL decision (Cases: Viacom et al v YouTube et al, 07 Civ. 2103 and The Football Association Premier League Ltd, et al v YouTube et al, 07 Civ. 3582, US District Court (S. District of New York), 23 June 2010, at page 15):

> *"The tenor of the foregoing provisions is that the phrases "actual knowledge that the material or an activity" is infringing, and "facts or circumstances" indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough. That is consistent with an area of the law devoted to protection of distinctive individual works, not of libraries. To let knowledge of a generalised practice of infringement in the industry, or of a proclivity of users to post infringing materials, impose responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA."*

More recently, in Telecinco (Telecinco et al v YouTube LLC, Commercial Court of Madrid, Judgment No.289/2010, 20 September 2010) the Spanish court cited with approval the Paris Court's decision of 15 April 2008, as follows (office translation):

> *"What this means is that actual knowledge must be proven in detail, mere suspicion or rational indicia not being sufficient to prove it. That definition of actual knowledge*

undoubtedly requires the cooperation of the injured party. This is rightly held by the judgment of the Tribunal de Grande Instance of Paris of 15 April 2008, which states that "actual knowledge of the clearly unlawful nature of a violation of the property or moral rights of authors or producers does not imply any prior knowledge and requires the cooperation of the victims of the infringement, who must inform the company which hosts the Internet users' sites of what rights they consider affected.""

Google submits that these court decisions correctly describe the knowledge requirement. There is a lack of definition of the term "actual knowledge" in many Member States implementing legislation and accordingly considerable scope for national variation in interpretation. We have experience of that, for example, in the German case Gisele Spiegel v YouTube LLC, Hamburg Regional Court, 324 O 565/08, 5 March 2010, mere flags by users on a video hosting service were held to constitute actual knowledge of illegality. Many Internet services put in place flag systems, allowing the user community to flag content that is not compliant with the terms of use and content policies. They receive a large number of flags, including some that may be malicious or spurious and in many instances, perfectly legitimate flags that relate to content that may violate a site's community guidelines, but not necessarily the law. Treating each as essentially a potential loss of the limitation of liability for the intermediary, would completely undermine the utility and value of flagging as an effective measure for an Internet intermediary to rely on their users' communities to flag inappropriate content. We have also encountered arguments that comments by users on content posted by others should fix us with actual knowledge, and that the lack of pre-screening and filtering should be a basis for criminal liability. None of this is helpful as it could call into question flagging systems or comments by users on content from others, which contribute to users' freedom of expression and involvement in the users' community.

Within Germany, there is no consensus about the term "actual knowledge". In several decisions, the Regional Court of Hamburg took into consideration whether the occurrence of infringements were to be expected with probability (e.g. LG Hamburg, 324 O 794/07 – *Weblog*; LG Hamburg 324 O 565/08). The court applied a much broader standard of being required to have knowledge and accepted that there should be a monitoring obligation:

> "*There is thus a "sliding obligation to exercise due care" with a graded range of monitoring obligations: If it is almost certainly predictable that an infringement of the right of personality will happen, the operator's monitoring obligation can increase to a continuing monitoring obligation or an advance monitoring obligation. The chamber does not mistake that the possibly arising monitoring obligation can impose a serious burden on website operators. The requirement of the above-mentioned sliding obligation to exercise due care ensues, in the chamber's opinion, from the circumstance that no legal asset can claim priority over the other in the constitutional consideration of freedom of opinion and press on the one hand and right of personality on the other."*

This, of course, appears to contradict the provisions of Article 15. In contrast, there are decisions in Germany that go the other way, holding that in view of the importance of hosting platforms for freedom of communications, a complainant should sufficiently substantiate his/her complaint - a simple hint should not be sufficient for the procuration of knowledge (the Higher Regional Court of Hamburg (decision 2 March 2010, Ref. 7 U 70/09), and the

Higher Regional Court of Cologne (decision 1 April 2010, Ref. 15 U 141/09)). Furthermore, the Higher Regional Court of Cologne did not think it impossible that the presentation of an affidavit may be questionable as proof of infringement. This kind of standard for actual knowledge is more akin to that described by the US and Spanish courts in Viacom and Telecinco discussed above and we suggest, is both correct and realistic.

This diverging interpretation of actual knowledge leads to severe legal uncertainty for the ISP. When and upon receipt of what quality of information does the intermediary have "actual knowledge"?

In relation to allegations of IPR infringement, there are things we will not know without sufficient information from others, for instance, the IPR holder or even a court determination. For example:

- What is the particular content in question and where exactly is it located? For instance, the URL and particulars of the content at that URL.

- Who owned/owns the IPR in that content? Not a trivial question - IPR are territorial, time-limited, licensed, etc, and there can be multiple IPR owners in relation to the same content. Indeed, we have encountered situations where one IPR owner asked for content to be removed, while another owner of IPR in the same content asked for it to remain on our service.

- Was that content provided by the user (uploaded, posted, transmitted, stored, etc) with the IPR owner's or owners' consent? In addition, does the user have other legal rights to enable them to do so - e.g. statutory rights to copy, rights to use a trade mark in the text of advertisements, or as a keyword within the limits of the test formulated by the CJEU, etc?

In the context of other types of illegality, often we do not know vital aspects. For example, whether an alleged defamatory statement is indeed defamatory of the claimant under applicable law and furthermore whether the user who published the statement had a defence, such as that the statement was true (truth being a defence in many countries). When considering the issue of actual knowledge it is also important to keep in mind that the level of legal uncertainty for intermediaries is aggravated by the fact that the same content can be deemed lawful or unlawful in different countries.

It is crucial that the term "actual knowledge" takes the above considerations into account. Notices should at the very least enable the intermediary to identify the complainant, locate the content (e.g. should include URLs), identify the alleged illegality and gather sufficient comfort that the content is indeed illegal. Indeed, this last point is expressly covered in the French and Portuguese implementing regulations - the principle being that the intermediary shall not be liable where the illegality is not obvious (Article 18). Notice of a problem, without specifying the nature of the illegality leaves the service provider in an impossible and impractical situation of testing the content under all possible areas of law and perhaps across multiple jurisdictions. The intermediary should not be forced to play the role of a court or competent authority in applying the law to the facts (both of which may be disputed) without a trial.

If intermediaries remove on defective notice (as regards the notice itself, see further below) without the above crucial ingredients - and we have seen other intermediaries take such an approach - then unidentified complainants may arbitrarily censor and restrict the availability of information to the public beyond their legal right to do so. Moreover, where complainants effect removals that do not fall within the specified circumstances permitted under Article 10 ECHR, then there will be an illegal breach of fundamental rights of Freedom of Expression.

In our experience, litigants (that is, claimants and potential claimants) prefer to provide only generic requests for removal and refer to broad categories of content (e.g. remove links to content that is defamatory of a person, or remove all clips of a certain TV programme series, without providing URLs). Typically, these requests are impossible to comply with.

Indeed, many litigants refuse to use our notice and take down procedures, including our state of the art Content ID system for YouTube which goes beyond the notice and take down requirements of the law.

Voluntary efforts to ensure that no illegal content is stored or transmitted require a level of activity by the intermediary (and are encouraged by the Directive, see for example, recital 40). For instance, a forum administrator who prevents offensive postings in a chat room, a hosting system that conducts manual review of flagged videos, an automatic assessment for risk of malware, a system to prevent notified trademark terms being use in ad text, and the creation and development of an advanced Content ID system for YouTube.

It is vital that these kinds of activities should not be interpreted as providing a basis for deciding that the intermediary is active, has knowledge of or control over the data stored and is no longer neutral, passive, automatic and merely technical, and therefore denied the benefit of the limitation. Otherwise, the intermediaries shall be incentivised and in some cases actively advised to take a hands-off approach - preferring to take the easier approach of doing nothing voluntarily - or else risk losing their limitation of liability.

There is a need to clarify that voluntary measures undertaken by responsible information society services to identify or prevent certain activities that may contravene applicable laws or the service's terms of use can in no case be considered as constituting "actual knowledge" and that only detailed, specific and complete notification should be considered as constituting the requisite knowledge. Furthermore, the notion of actual knowledge must refer to human knowledge (knowledge of an appropriate natural person within the specific service provider) and not "computer knowledge" whatever that expression may mean.

54. Have you had any difficulties with the interpretation of the term "expeditious" in Articles 13(1)(e) and 14(1)(b) with respect to the removal of problematic information?

Yes. In many countries, there is no express time limit and general principles of law would apply to the interpretation of "expeditious". However, in a few countries, there is an express time period. For example, in the Hungarian implementation 12 hours is mentioned and in the

Lithuanian implementation one working day after the user fails to reply to the intermediary, but both these deadlines are set in the context of a detailed take down procedure code.

In our view it is unworkable to specify a short time period, not least because of the wide variety of information society services that exist and that may be developed. Instead, the flexible approach of the majority of MS legislators is appropriate in this regard - which we consider to be consistent with the technology neutral approach to the legislation.

Some examples may help to illustrate the point. In Germany:

- The Regional Court of Cologne demanded in its decision of 12 August 2009, Ref. 28 O 705/08, a “prompt restriction and deletion” of unlawful contents after knowledge, the knowledge allegedly existing due to an (earlier) complaint.

- On the other hand, the Higher Regional Court of Cologne in appeal proceedings with its decision of 1 April 2010, Ref. 15 U 141/09, did *not* aim for the time of the first complaint or warning, but instead referred to the date of service of the injunction regarding the relevant information. However, service of the injunction in this case took place six months after the first complaint!

As the examples show, even according to the courts, there may be months of difference between the points in time where the service provider should react.

Many of our removal procedures require manual input and engineering effort. One cannot simply press a button and remove precisely what each complainant desires. Sometimes, for controversial content the intermediary needs to exercise human judgment, discuss internally, obtain translations where complaints are in other languages and even seek legal advice, before making an informed decision. Sufficient time needs to be afforded to permit service providers to make considered, reasoned decisions. In addition, many complainants do not appreciate the technical challenges involved, including implementing and migrating changes over thousands of computer systems, perhaps worldwide and there may be large technical differences between services even where provided by the same intermediary.

Time should only start running from the moment when the information society service in question has actual knowledge that the content it illegal, not before that moment - as explained above, in many cases, the illegality of the activity is not apparent from the notice and/or the content to be removed is not sufficiently identified. Then, after time has started running, “expeditious” should mean that the information society service moves without undue delay to make the changes to initiate the removal. However, because of the technology and size of the task involved, the removal may not actually occur for some time. In some cases it can take days for the removal to take full effect. Therefore, a flexible approach to “expeditious” is necessary and justified.

55. Are you aware of any notice and take-down procedures, as mentioned in Article 14.1(b) of the Directive, being defined by national law?

We assume that this is a typographical error and the question should refer to Article 14(3).

Most Member States do not have such procedures. However, we are aware that there are procedures set out in implementing legislation or codes of conduct in (at least) Finland, France, Hungary, Iceland, Lithuania, the Netherlands and Portugal. Each involves the complainant sending a notice to the intermediary. Some require the intermediary to forward the notice to the user, though this may happen before (e.g. Lithuania) or after (e.g. Hungary) the intermediary takes action to remove the allegedly illegal content.

In our view, a well-thought out notice and take down procedure that is uniform across the EU (indeed EEA) would be extremely useful for all stakeholders. It would facilitate the removal of illegal content, safeguarding the rights of complainants, users and intermediaries. We submit that there are a number of central principles which should apply to such a procedure. We identify those requisite principles as follows (currently, none of the existing procedures seems to include all of them):

(1) Before approaching the intermediary, the complainant should make a reasonable effort, making use of the means and information publicly available, to contact the user in question to have the objectionable content removed. This would also help to educate Internet users to understand that they are effectively responsible and liable for the content that they post online. It is also useful in preventing complainants from initiating knee-jerk, immediate action against intermediaries, who are not the persons responsible for originally providing the content.

(2) There is no liability on the intermediary where none exists under applicable law. See the discussion on this under Q52 point 4.

(3) In all notifications, the complainant must give sufficient information. This is probably best achieved by specifying the requisite information that the complainant's notice must contain.

(4) If: (a) the notice is not received; or (b) the notice does not provide the requisite information; or (c) the illegality is not obvious; then there should be no liability on the intermediary. See for example, Article 18 of the Portuguese implementing legislation and Article 15 of the Icelandic implementing legislation.

(5) The intermediary must be permitted, where it able to do so and without liability, to forward the notice to the user in question. In this regard, see the Commission's Study of the Liability of Internet Intermediaries 2007, page 16.

(6) That user should have an opportunity to send an objection to the complainant.

(7) Upon the intermediary receiving actual knowledge, that is, when the content and the illegality are precisely identified and the illegality is obvious, the intermediary should take expeditious action to remove the content, but not before that point in time. Guidelines will be needed in relation to "illegality is obvious" otherwise national divergences will result. This means that both the complainant's notice and the user's objection need to be evaluated. Where no potential liability on the intermediary exists under applicable law (see (2) above), it should be clarified that the intermediary need not remove the content.

(8) The intermediary is not the appropriate person, nor must it be forced, to play the role of judge. Where illegality is not obvious, a cheap and convenient way to assess illegality is required. In our view, it is unnecessary to burden the courts with this. Therefore, we suggest the utilisation of an ADR mechanism to assess illegality. The ADR mechanism must trigger quickly and while it is engaged the intermediary should take no further action and have no liability accruing to the complainant or the user.

(9) In view of the wide range of information society services all time limits, if any are imposed, must be realistic, reasonable, flexible and workable, to take due account of all actual constraints linked to the removal.

(10) In addition, there should be no liability on the intermediary where it acts in good faith to follow the notice and take down procedure.

56. What practical experience do you have regarding the procedures for notice and take-down? Have they worked correctly? If not, why not, in your view?

For many years, we have had copyright notice and take down procedures for our services. See for example, http://www.google.co.uk/dmca.html (setting out our DMCA-style notices) and http://www.youtube.com/t/copyright_notice (describing the YouTube content management procedures, including our state of the art Content ID system). The important experience gained is valuable. At the outset, we would point out that these systems have been used successfully by complainants all over the EU. Small issues, like complainants giving insufficient information arise fairly frequently, and we endeavour to rectify them by asking the complainant for the missing data (for example, by referring to our own forms for notice). This supports our view that an EU-wide common form of take down notice would be highly beneficial.

However, it is frequently the case that litigants, that is claimants and potential claimants, are reluctant to use our notice and take down procedures. It often appears that they do not actually want the content removed. Even when encouraged to use our notice and take down procedures by the court, the litigant may hinder the process - for example, by sending us photocopied lists of URLs as opposed to editable versions, thus forcing us to re-type every URL input manually; refusing to use our automated notice systems optimised for bulk notifications; and hampering the provision of video data for use in our Content ID systems. In addition, many litigants refuse to particularise the content that they allege infringes their rights. They consider that this is not something that they should do. Despite Article 15, they believe that the intermediary must locate the content that infringes their rights. Apart from the clear policy issues involved here, for many reasons, including those given in Q53 above, this kind of search would be impossible for the intermediary. For more on this, please also see the question on filtering at Q58 below.

There are problems arising from the fact that content may include various works owned by different owners, or indeed, alleged owners. We have experience of situations where one alleged copyright owner requested a video to be removed, while another alleged copyright owner wanted it to stay on the service. This puts the intermediary in an impossible position, and at risk to be held liable by one side or the other depending on the action or inaction that it takes (please see the principles set out in answer to Q55 above).

In relation to our trade marks complaint procedure for AdWords, our policies and complaints procedure have been refined along the years to reflect case law and clarification of the exact scope of trade mark rights.

Where the illegality is unclear, there may be difficulties. It may be that neither the user in question nor the intermediary agrees to remove the content and the claimant sues either the intermediary or the user or both. The geographical extent of removal sought by the complainant may be a central part of the dispute - involving both technical and legal considerations. For the EU to obtain the benefit of e-commerce, information society services must be able to cross borders, grow and operate at scale. It is exceedingly difficult to operate a notice and take down procedure on the scale required in the face of voluminous, ambiguous claims of illegality that require significant nuanced considerations, perhaps over more than one country's laws. Ideally, information society services would be spared the burden of making these kinds of determinations by the ADR mechanism referred to above.

57. Do practices other than notice and take down appear to be more effective? ("notice and stay down", "notice and notice", etc.)

Notice and take down has severe shortcomings associated with it. For example, such a system leads to over-broad removals and is open to abuse. This is even more likely where intermediaries adopt a very cautious approach, not questioning anything about the complainants claim or considering the user's position - and SME intermediaries may well have no other option. Complainants will be able to remove or indeed censor content without due scrutiny and legal safeguards. In particular, there would be no effective mechanism for the user's position to be taken into account.

Notice and stay down also has severe problems associated with it. Firstly, it is technically problematic - removing certain content and stopping it from re-appearing represents massive challenges. Indeed, it is not a practical, working, viable, technical option at all in many situations.

Secondly, stay down systems are technology and service specific. For YouTube, we have developed the state of the art Content ID system that can, within technical parameters, identify matching video clips. Using these systems, copyright owners can locate copies of their works, choose to remove them, track them, or generate a new source of income by allowing ads to be placed against them. However, this system requires the active participation by rights holders to work and even then, the provision of good quality samples of the complainant's content to function effectively and it is only for YouTube. While an increasing number of rights owners including major US network broadcasters, movie studios and record labels are using the system, some complainants simply do not want to collaborate for this purpose. Notice and stay down becomes unworkable when there is no known technical or practical way to find classes of content that the complainant would consider to be repeat content.

Thirdly, and perhaps most importantly, forcing intermediaries to implement notice and stay down regimes, technologies and systems, would be a huge barrier for new, small and start up intermediaries.

Fourthly, notice and stay down directly contradicts the no obligation to monitor principle set out in Article 15, because it forces intermediaries to permanently monitor all content uploaded by users in order to stop the content from re-appearing on their services.

Fifthly, since the intermediary does not control what users do, the intermediary can be in breach of a stay down order without realising it.

Notice and notice - uniformly applied across the whole of the EEA - may be a workable scheme for intermediary services, in light of all the above and the procedures set out in certain MS implementing legislation. It would be a notice and objection procedure embodying all the principles numbered (1) to (10) set out under Q55 above, where the intermediary agrees to act in accordance with the decision of the ADR mechanism.

The basic structure could be: complainant contacts the user, if no response, complainant sends notice in due form to intermediary. If the notice is in due form and the illegality is particularised and obvious, then the intermediary removes. Otherwise, the intermediary forwards the notice to user and is entitled to wait, without liability, to allow the user to file an objection. Alternatively, the user may fail to reply. The complainant sends the notice and objection (or failure to reply) to the independent ADR mechanism for a quick decision on the dispute between the complainant and the user. The intermediary acts in accordance with the ADR decision (removes or leaves it up). Intermediary shall not be liable where they follow the procedure in good faith (and the intermediary would not be liable in any event, unless they have liability under applicable law).

58. Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations?

Yes, there is currently an intense struggle between various stakeholders in this crucial area. What happens next is of fundamental importance to the future of the Internet, the availability of information society services in the EU, human rights and fundamental freedoms. Before mentioning specific cases, we would like to first explain some key concepts.

One of the cornerstones for information society services is set out in Article 15. It is worth reiterating why it is so fundamentally important. The principle is that intermediaries have no general obligation to monitor the information that they transmit or store nor a general obligation to seek facts or circumstances indicating illegal activity. This principle is vital for information society services to flourish and the Internet to work. Without it, many services that exist today would not be possible.

If intermediaries had to ensure that they knew about everything they store or transmit, it would be necessary for them to check and assess all information supplied by users of their services. They would then have to verify the legal status of everything and this would be in all fields of law. If not impossible such monitoring would at least be so complex that it would threaten the very function of the intermediary, since in effect they would no longer be able to allow things to be put online which is a vital ingredient to the richness and very existence of the Internet today. Indeed, the ability for users to post online without monitoring is a fundamental feature of the Internet. For many services, the sheer volume and enormity of

general monitoring renders it impossible. Every minute, YouTube users upload more than 24 hours of video content to the hosting service. In other words, every day, approximately 4 years worth of new video is added, from all over the world. Services like YouTube could not exist if the intermediary had to monitor on such a grand scale and in relation to all known laws.

It would not only be impossible, but would lead to the obvious risk of private censorship[5] which is prejudicial to freedom of expression[6]. At extreme, the danger is that the information society would revert to a world where only a limited number of enterprises control the editorial content consumed by society.

It is worth underlining that the "no obligation to monitor" principle is necessary for the limitations in Articles 13 and 14 to work. If the intermediary had a general obligation to monitor, then they are more likely to be held to have actual knowledge for all content, rendering the limitations pointless and useless.

The current structure therefore, is that intermediaries do not have to *proactively* check content, but only to *react* promptly from the moment they actually have the requisite knowledge.

On the other hand, courts are able to make orders requiring the intermediary to terminate or prevent infringement (Articles 12(3), 13(3) 14(3) and in relation to intellectual property Article 11 of the Intellectual Property Rights Enforcement Directive 2004/48/EC ("IPRED")).

Clearly a tension exists. When does an order to prevent infringement amount to (an illegal imposition of) a general monitoring obligation? There is a major struggle between rights holders and intermediaries on these issues.

In relation to non-Google cases, crucial questions are currently on reference to the CJEU in at least three cases (L'Oreal v eBay C-324/09 (from the UK High Courtt), SABAM v Scarlet C-70/10 (from the Brussels Court of Appeal) and SABAM v NetLog C-360/10 (from the Brussels Court of First Instance).

[5]This risk was also pinpointed by the Committee of Ministers of the Council of Europe which, in its declaration of 13 May 2005 on human rights in the information society invited the Member States to tackle the following problem *"censorship (hidden censorship) by private service providers of Internet services, for example the blocking or elimination of contents on their own initiative or at the request of a third party – final CM(2005)56 13 May 2005, Section II §3*"

[6]The forty-sixth recital of the Directive mentions in this respect that the storage service providers must not adversely affect the freedom of expression: "(46) *In order to benefit from limitation of liability, any service provider of a service of the information society consisting of data storage must act promptly to withdraw the information concerned or make access to it impossible immediately he actually becomes aware of or realises the illegal nature of the activities. The information must be withdrawn or access to it made impossible* ***with due regard for the principle of freedom of expression*** *and the procedures laid down for this purpose at national level.*"

In recent proceedings for Judical Review, BT and TalkTalk argue that the UK Digital Economy Act 2010 includes provisions that amount to a general monitoring obligation in breach of Article 15.[7]

In addition, in our experience, claimants do obtain orders, sometimes in camera (private and ex parte hearings), to remove allegedly illegal content that are impossible to comply with. We have many examples of this, but for the sake of discussion, here we consider only two of them. The first, a restrictive injunction directed towards an intermediary along the following lines (X and Y v. Z and persons unknown):

> *"...the defendants...must not...defame...the claimants... by publishing on the Internet or by any other means whatsoever allegations of [details specified]"*

The second example is from the RTI case in Italy, regarding an interim injunction in relation to YouTube (office translation):

> *"Orders to the defendants – directly or also through third parties controlled by them – the immediate removal by their servers and the consequent immediate disabling the access to all the content reproducing fixed or moving images' sequences concerning the TV show "Grande Fratello", tenth edition [Italian Big Brother 10];*
>
> *Prohibits the defendants from continuing the infringement of the utilisation and economical exploitation neighbouring rights of the TV show at issue;"*

It could be said that such injunctions are typical of those ordered against a wrongdoer or infringer. They are not apt for intermediaries. For an intermediary, injunctions such as the above are impossible to comply with without the collaboration of the claimant. We do not know what content infringes their rights or is defamatory of them (or is true, for example) and where it is located. We are not in control of what users do and accordingly may be in breach of such an order without realising it, with no knowledge of the particular content. Anyone may upload defamatory or copyright infringing content and thus put us at risk of being in breach of the order. By "anyone" we do mean any person, including the claimant, his or her agents or parties connected with the claimant. In general terms, such an order is open to abuse (including by the claimant), who may be motivated by a desire to enhance their claim for money damages.

In the first example we vigorously defended the matter and the litigation ended soon afterwards. In the second example, we unsuccessfully appealed against the form of order and the case continues on the merits.

In other cases, claimants have asked for specific filtering measures to be implemented on our service (for example, Bayard Presse v YouTube) while at the same time refusing to collaborate and use YouTube's video identification system. The theme that we see is a

[7] See their Statement of Facts and Grounds available here (at paragraph 140ff): http://www.btplc.com/News/Articles/Showarticle.cfm?ArticleID=98284B3F-B538-4A54-A44F-6B496AF1F11F

common one: rights holders want YouTube to prevent any upload of their content without precisely identifying it. They consider that it is for YouTube to know the rights holders' catalogs and proactively identify what is uploaded by users to the platform.

In Germany, there is additional legal uncertainty as a result of the doctrine of "interferer liability" (*Störerhaftung*). The BGH established criteria for interferer liability in relation to Internet auction platforms (e.g. the infamous eBay and Ricardo decisions) and held that the auction site should be considered an "interferer". It was not only obliged to remove the individual infringing content, but also to take measures to avoid future infringements of the same kind. With this, the BGH established far reaching obligations on Internet auction platforms in Germany, which appear to conflict directly with Article 15. The manner in which this doctrine has been applied by various courts with respect to different Internet services has been far from uniform. For instance, some decisions have generally opposed monitoring obligations directed towards the future (e.g. Ref. 17 O 287/07, 29 May 2008), whereas others have granted injunctions against the service provider that amount to comprehensive monitoring obligations for the future of nearly indeterminable extent (e.g. Ref. 28 O 705/08, 12 August 2009).

In sum, orders should not be made that the intermediary is incapable of complying with and in particular, orders should not be made that breach Article 15. No doubt the CJEU may clarify some issues in this area in the three references before it. However, we suggest that guidance would be helpful on the kinds of injunctions that ought not to be ordered against intermediaries, to assist courts in interpreting Article 15 against the other provisions cited above.

59. From a technical and technological point of view, are you aware of effective specific filtering methods? Do you think that it is possible to establish specific filtering?

Google's belief is that the development of innovative content services that meet consumers' expectations and needs is the most effective way to prevent infringement and value copyright online. In this context, Google considers that business and technological innovation has much more to offer than filtering measures simply meant to block access to content. Technological developments should be used to improve users' access not to restrict it.

The evolution of YouTube illustrates how technological and business innovation can increase users' access to online content and allow rights holders to monetise this access. YouTube makes use of content identification technologies to foster online access to content, not to restrict it. This approach creates a real incentive for content hosting platforms and rights holders to collaborate. On the one hand content hosting platforms have an incentive to develop and maintain truly efficient solutions to identify protected content. On the other hand rights holders have an incentive to collaborate to the development of such solutions, and to make their content available online. Such collaboration can only be developed on a voluntary basis, in the context of the legal framework defined by the e-commerce Directive. The use of content identification technologies can at best allow the identification of copyright protected content that have been identified as such by the rights holders. However, they cannot make the distinction between an unauthorised use of a copyright protected content,

and the legitimate use of this content by users falling under the scope of a copyright exception or a licence.

Accordingly, the use of technologies to identify copyright protected content cannot give rise to a presumption of actual knowledge that would expose Internet intermediaries to liability. Instead, the legal presumption should remain and ultimately it would be for the rights holder to provide a precise notice to the intermediary of any copyright infringing content that should be removed.

While technologies allowing identification of protected content at the level of services may be used to foster innovative content services, the application of filtering measures at the level of communication networks, may well achieve the opposite result. The application of filtering technologies would suppose that Internet access providers actively monitor their networks. While the technical feasibility or efficiency of such a monitoring is actually doubtful and contested [4], the use of filtering technologies entails important risks for the development of information society services.

Packet-filtering and analysis is a process that requires a large amount of processing power and network reconfiguration. It risks degrading the quality and users' experience for perfectly legitimate online services, raising serious concerns for competition and innovation. It also risks preventing legitimate uses of copyright protected content, and negatively affects the development of user-driven creation. In addition, filtering risks imposing high cost on consumers and negatively impact on the uptake of broadband access.

Additionally, there are reasons to believe that filtering will not achieve much in preventing copyright infringement online, with the ability for users to encrypt their communications rendering filters totally ineffective. Experience has proven that technical systems meant to restrict access to content, have largely failed to address the problem of online copyright infringement.

The feasibility, effectiveness, costs, or real impact of filtering technologies at the level of communications network, is subject of much speculation at the moment. In this context, Google assumes that the European Commission will not take any position on filtering, and its effectiveness to actually "prevent online infringement" before leading an in-depth and well documented analysis on its potential economic, technical and societal impact.

Such assessment should take into account the real costs, effective benefits, and actual risks raised by the application of filtering at the level of network, as well as its likely effects on innovation, creation, and the development of the Information Society in Europe.

60. Do you think that the introduction of technical standards for filtering would make a useful contribution to combating counterfeiting and piracy, or could it, on the contrary make matters worse?

Before considering standards for filtering and the impact of the standardisation of such technology, it is key to consider the technological feasibility of such systems as well as their legal, societal and economic impact, and their potential to effectively achieve or undermine Europe's objectives and core values.

In addition, a fairly obvious observation must be made. As soon as there is such a technical standard, then unscrupulous users will try to find ways to circumvent it and history indicates that they are are likely to succeed.

That said, the cost to develop, deploy, maintain and operate these kinds of systems are enormous and after all that, the results are uncertain. In any event, this sort of activity can only be undertaken by large organisations with significant resources. Requiring this would discourage the seeding and growth of entrepreneurial activity within Europe.

61. Are you aware of cooperation systems between interested parties for the resolution of disputes on liability?

Our co-operation procedures, for example, the DMCA style notices, anti-counterfeit procedures for AdWords, trade mark complaints procedures for AdWords, and the YouTube Content ID system, are all notice-based systems. In our replies to Q55 and Q56 above, we have explained the basis for our view that ADR mechanisms could play a huge and useful role to resolve disputes between rights holders and users in assessing the illegality of content.

Liability for the intermediary however, is a separate issue and we refer to our answer above at Q55 and principle (2). Only the legislators and the courts may decide whether an intermediary should be liable in particular circumstances.

62. What is your experience with the liability regimes for hyperlinks in the Member States?
63. What is your experience of the liability regimes for search engines in the Member States?

We shall answer questions 62 and 63 together. Hyperlinks are a central feature of the Internet, being a characteristic of the programming languages and technology involved, such as HTML. Links can take various forms, typically text (often blue) and images (for example, thumbnails). Everyone who uses the Internet and information society services may be a “hyperlinker”. For example, an email user, a blogger, a user of a word processing service, can easily create a hyperlink in just a few clicks. Accordingly, it is important to bear in mind that when speaking of hyperlinkers, the phrase covers in essence all “users”, that is, the public at large.

Search engines serve a crucial function in the information society, as has been recognised by various courts around the EU. Hyperlinks are an important part of search results. Likewise, many other information society services provide hyperlinks (e.g. Twitter). So, while users are providers of hyperlinks, so are search engines and other information society services.

It is submitted that the law in this area is in tatters. Harmony across the EU is non-existent. There is no clarity for users, information society services or the courts. Consider the following from case law and legislation:

The Advocate General of the CJEU considered, correctly in our view, that the Google web search engine was an information society service under the e-commerce Directive. He thought it was probably covered under the caching provision, Article 13 (paragraphs 136, 144 and footnote 72, C-236/08 to C-238/08).

In relation to an allegation for copyright infringement by Copiepresse against the Google News Search, the Brussels court considered that the e-commerce Directive was not relevant (Copiepresse et al v Google Inc., Brussels court of first instance, RG 06/10928) (In a similar allegation by Copiepresse against the European Commission's own news service, we understand that the court dismissed the claim for jurisdiction reasons).

The Bundesgerichtshof considered Google Image Search to be covered under the hosting provision (Thumbnails case cited above).

The UK High Court (civil), considered that search engines are information society services (Metropolitan Schools, cited above at paragraphs 55 and 84):

> *"A search engine, however, is a different kind of Internet intermediary. It is not possible to draw a complete analogy with a website host. One cannot merely press a button to ensure that the offending words will never reappear on Google search snippet: there is no control over the search terms typed in by future users. If the words are thrown up in response to a future search, it would by no means follow that [Google] has authorised or acquiesced in that process."*
>
> *"Although the matter is by no means free from doubt, it would appear on balance that the provisions of the 2002 Regulations are apt to cover those providing search engine services."*

The High Court went on to say:

> *"The United Kingdom has, to date, not chosen to extend the Regulations expressly to cover search engines. This would appear to be on the basis that no cases have emerged suggesting that such a protection is necessary. The position may well be reconsidered if the European Commission publishes a further review."*

In relation to a provider of hyperlinks, the UK Crown Court (criminal) considered that the "mere conduit" provision (article 12) could provide a complete defence to a charge of criminal copyright infringement (TV Links).

In contrast, for example, is a decision of the Higher Regional Court of Munich of 23 October 2008 29 U 5697/07 (*AnyDVD*). A press company wrote an online report about certain copy protection circumvention software (AnyDVD of company Slysoft) and the problems relating to it under copyright law. The press company's reporting was objective. Aside from many other hyperlinks, for instance a link to the German copyright legislation, the press company included a link to the homepage of the company Slysoft. The Higher Regional Court confirmed the lower instance decision that the German "interferer" doctrine should apply. Accordingly, the Higher Regional Court assumed that the inclusion of the hyperlink

supported a claim of copyright infringement against the press company. The case was appealed to the final appeal court, the BGH, and its decision is anticipated soon.

In addition, there are cases around the EU suggesting that the text in a hyperlink itself may amount to a copyright infringement (similar issues to those being discussed in Infopaq C-5/08).

The national implementing legislation position is as follows (as far as we have been able to understand):

Search engines are expressly covered under provisions similar to “mere conduit” in national implementing legislation in Austria, Bulgaria and Liechtenstein.

Search engines are expressly covered under provisions similar to “hosting” in national implementing legislation in Hungary, Portugal, Romania and Spain

In Finland, Norway, Sweden, the Netherlands and Iceland: the implementing legislation does not expressly mention search engines, but the government bills indicate that the legislators intended to include them.

Hyperlinks are expressly covered under provisions similar to “hosting” in national implementing legislation in Austria, Liechtenstein, Portugal, Romania and Spain.

As can be seen from the case law and legislation above, providers of hyperlinks are apt to be covered by one or more of articles 12 or 14. Search engines are apt to be covered by one or more of articles 12, 13 and 14. It is hardly surprising that courts have taken a pragmatic approach.

To foster some level of harmony across the EU, encourage a flourishing information society, nurture innovative Internet services and prevent national barriers, some form of guidance is required. The guidance could simply confirm once and for all that: (a) both providers of hyperlinks (including embedders) and search engines fall within the definition of information society services (see for example the Commission Proposal 1998 (at pages 7 and 14) and recital 18 in the Directive); (b) where express national implementing provisions exist, they should be applied; and (c) if no such express national provisions exist, then providers of links may be covered under one or more of Articles 12 and 14, while search engines covered under one or more of Articles 12, 13 and 14 as the per the facts and circumstances in each case.

There are billions of websites, numbers are increasing exponentially and geographically. Users need a way to find information that is of interest to them. Search engines perform a highly important function in the information society. Arguably, this justifies putting them in a position of special protection. Using algorithms, a search engine produces snippets of content based on a combination of the user’s query and indexed information. The complainant always has recourse to the site that contains the information that they complain of. They ought to seek redress that way and there are important reasons to encourage that (see principle (1) under Q55 above). Where the site removes the information, then that is reflected in later search results, as the search engine index automatically refreshes. Search

engines are neither in control of users nor the enormous numbers of third party sites. Moreover, the search results themselves may not be illegal in any way. It is clear therefore, that the search engine's position is further removed from that of a host, and accordingly, treating search engines under hosting type provisions is not the best option. Otherwise, complainants are encouraged to go directly to the search engine to solve their problems, which has the effect of restricting the availability of information for all and increasing the risks of private over-censorship and negative impact on freedom of expression (see above for discussion of these topics).

In absence of existing legislation and in line with liability regime already applying in Austria, Bulgaria and Liechtenstein, of the three existing provisions in the Directive, we suggest that the best approach would be to issue guidance that search engines should be considered under provisions similar to mere conduit (Article 12), and that any further national legislation in this field should follow this approach.

64. Are you aware of specific problems with the application of the liability regime for Web 2.0 and "cloud computing"?

The phrases Web 2.0 and cloud computing capture such a diverse range of products and services, and are so arbitrary, that it is not possible to answer on "specific problems". However we would like to point out three issues here:

- The development of Web 2.0 or participative web is giving rise to an exponential development of user-created content, with the possibility for users to post videos, blog posts, pictures or comments (see some of the figures cited above). For users, the possibilities offered by Web 2.0 support creativity, social interaction, freedom of expression and the Internet as we know it. For intermediaries this creates a situation where they do not deal with a limited number of professional web publishers anymore, but all Internet users who now have the possibility to post content online. This reinforces the need for robust ISP liability limitation under the e-commerce Directive, as intermediaries simply cannot be held accountable directly for the acts of any users, or be required to police them and make decisions on what should be allowed and what should not.

- Web 2.0 and cloud computing lead to the development of complex services involving different activities. This is a consequence of the healthy and natural evolution of technology and the information society from that envisaged in the late 1990s. As a result, and as pointed out in the answer to Q52, it is important to make a separate assessment of the different intermediaries activities in a given service. So for example, when it comes to hosting it is vital that the focus is on the allegedly illegal content and whether the host's activities in relation to that content were limited to storage of the information. There is a need for a flexible interpretation of the activities defined in article 12 to 14. For instance, while the criteria that define hosting activities are very suitable for traditional services, their weakness become apparent when applied to cloud computing or Web 2.0 services. Technological evolution calls for flexible interpretation.

- The fast pace at which Web 2.0 and cloud computing developed demonstrate the need for technology neutral approach when considering ISP liability limitation. Innovation is so rapid, that any other approach is likely to be doomed to fail.

65. Are you aware of specific fields in which obstacles to electronic commerce are particularly manifest? Do you think that apart from Articles 12 to 15, which clarify the position of intermediaries, the many different legal regimes governing liability make the application of complex business models uncertain?

Each country has its own laws. Despite the honourable attempt to implement the country of origin principle in the e-commerce Directive, a real benefit in practice has not materialised because the regime expressly excludes many important fields of law that are almost always implicated in e-commerce, most notably intellectual property and data protection. As a result much remains to be achieved if Europe is to create a vibrant Digital Single Market. In particular, guidance is needed to ensure that data protection law should be interpreted in a manner that is consistent with the e-commerce Directive and vice versa. Serious inconsistencies between the two bodies of law would wreck further growth and development of the information society in Europe.

66. The Court of Justice of the European Union recently delivered an important judgement on the responsibility of intermediary service providers in the Google vs. LVMH case. Do you think that the concept of a "merely technical, automatic and passive nature" of information transmission by search engines or on-line platforms is sufficiently clear to be interpreted in a homogeneous way?

We believe that it is not, and that guidance is required. This wording is from recital (42) of the e-commerce Directive. In other words, it is not in the operative part of the Directive. It is abundantly clear that there is plenty of scope for recital 42 to be applied in a non-uniform manner in different courts across the EU.

For example, presentation and display are not mentioned in the wording of Article 14, yet, the Hamburg court held that certain videos uploaded to YouTube by users should be treated as content appropriated and provided by YouTube itself and not covered by Article 14 ("zu eigen machen") Peterson v Google Inc and others, Hamburg Regional Court, 308 O 27/09, 3 September 2010. In essence, the host limitation of liability was not available to YouTube because of way in which user generated content was presented and displayed. This is in direct contrast to the opposite conclusion in Telecinco, a decision handed down by the Spanish court shortly after the Hamburg court ruled in Peterson.

Another example is that the words "mere storage" do not appear in Article 14, but some courts have interpreted the provision that way. In Kaschke, a website owner was sued for defamation in relation to user generated content posted on to his website. The website owner argued that he had no effective control over the person who posted the alleged defamatory words, that he did not monitor the site and as soon as he became aware of the claimant's complaint about posting, he removed it and offered the claimant a right of reply. However, the UK High Court decided that the website owner was unable to rely on the Article 14 limitation and stated (bold added):

> *"...[the website owner] exercised some editorial control on parts of the website and in particular on the homepage. It is quite clear from his evidence that his involvement in*

*the website as a whole and in particular in the **homepage** went beyond the **mere storage** of information."*

Virtually every website owner controls the appearance of their homepage and exerts control on at least part of their site. For example, Google arranges its web search homepage in a particular way, occasionally with a Google Doodle above the search box. That cannot and should not affect our liability position for content that advertisers create in their AdWords ads for example. Generally, editorial or layout changes by an information society service should be permissible without the service losing its limitation of liability protections.

The Kaschke decision also suggests an answer to the issue (as discussed under Q52 above) namely that the granularity, focus and flexibility required when applying the hosting provision may be achieved by concentrating on the host's activity in relation to the allegedly illegal information:

"However in my judgment that is not determinative of the question raised on this aspect of the appeal because it still does not necessarily identify the information society service whose provision is referred to in [Article 14]. Is it the storage of the particular information provided by the particular recipient of the service the storage of which results in the liability which would exist but for the exemption conferred by [Article 14], or is it the storage of all the information which is provided by all recipients of the service?"

After considering the legal arguments, the Court decided (at paragraph 75):

"...the question to be asked is whether the information society service provided by the defendant in respect of the information containing the defamatory words which would otherwise give rise to liability consists only of and is limited to storage of that information. If the answer to that question is that it does consist only of storage of the information, [Article 14] immunity is potentially available even if it would not be available in respect of other information also stored by the defendant in respect of which the service provided by the defendant goes beyond mere storage."

In other words, consider the specific information containing the allegedly illegal content and ask: "was the information society service provided in respect of that information limited to the storage of that information?" If "yes", then the hosting limitation of liability is potentially available to the information society service (subject to satisfying the extra conditions).

This approach provides way for the limitation of liability provisions to work effectively with modern, rapidly evolving, Internet services. It should be case by case (as mentioned by the ECJ in cases C-236/08 to C-238/08) and specific as discussed above.

This discussion also underlines the points made above, that voluntary systems for notice and take down, flagging systems, manual review systems, aimed at preventing illegal content or content that violates terms and conditions of service, should not be counted when considering whether an intermediary is passive, merely technical, automatic, etc. Otherwise, the intermediary is incentivised to do nothing, rather than try to do something, because by

doing something, they may lose the benefit of the limitations on liability set out in the Directive.

Voluntary efforts to ensure that no illegal content is stored or transmitted require a level of activity by the intermediary (and are encouraged by the Directive, see for example, recital 40). For instance, a forum administrator who prevents offensive postings in a chat room, a hosting system that conducts manual review of flagged videos, an automatic assessment for risk of malware, a system to prevent notified trade mark terms being use in ad text, the creation and development of an advanced Content ID system for YouTube.

It is vital that these kinds of activities should not be interpreted as providing a basis for deciding that the intermediary is active, has knowledge of or control over the data stored and is no longer neutral, passive, automatic and merely technical, and therefore denied the benefit of the limitation. Otherwise, intermediaries shall be incentivised to take a hands-off approach - preferring to take the easier approach of doing nothing voluntarily - or else risk losing their limitation of liability. The encouragement of a hands off approach also has the added undesirable effect of stifling innovation, for example, in crucial fields of illegal content detection.

67. Do you think that the prohibition to impose a general obligation to monitor is challenged by the obligations placed by administrative or legal authorities to service providers, with the aim of preventing law infringements? If yes, why?

Please see our answers to Q58 and 59, where we have underlined why this prohibition is important for the information society to flourish in the EU and explained some of the issues we are aware of, including in relation to widely drafted court orders, and discussed filtering. In addition, we would make the following observation. Larger intermediaries generally have the resources to comply (subject to some of the challenges discussed throughout our response) with administrative and legal authorities which adopt a reactive and specific approach in line with Article 15. In order to enable and encourage new entrants to become Internet intermediaries, obligations imposed on them must be realistic, pragmatic and achievable including in terms of both time and cost.

68. Do you think that the classification of technical activities in the information society, such as "hosting", "mere conduit" or "caching" is comprehensible, clear and consistent between Member States? Are you aware of cases where authorities or stakeholders would categorise differently the same technical activity of an information society service?

Inconsistencies in the classification of activities have been discussed above, for example, the national divergences in interpretation of hosting for video platforms in Q52 and in response to other questions. A further example of that situation was the AdWords system. Prior to the CJEU decision in cases C-236/08-238/08, the Strasbourg Court (in Atrya v Google, 20 July 2007) had held that the AdWords system was covered under the hosting provision, whereas other French courts had taken the opposite view.

Clearly, there is a need for a flexible interpretation of the activities defined in article 12 to 14. While the criteria defining hosting activities are very suitable for traditional services, their

weakness become apparent when applied to cloud computing or Web 2.0 services. Technological evolution calls for flexible interpretation.

As a result, and as pointed out in the answer to Q52, it is important to make a separate assessment of the different intermediaries activities in a given service. For example, when it comes to hosting it is vital that the focus is on the allegedly illegal content and whether the host's activities in relation to that content were limited to storage of the information. This approach may provide the granularity, focus and flexibility required for the limitation of liability provisions to work effectively with modern, rapidly evolving, Internet services.

69. Do you think that a lack of investment in law enforcement with regard to the Internet is one reason for the counterfeiting and piracy problem? Please detail your answer.

Rights holders play the central role in enforcing their rights as they are in a unique position to determine their rights and when their rights have been infringed. As pointed out in the answer to Q57, our notice and take down procedures for copyright and trademarks are meant for and used by rights holders to enforce their rights. We do not have any element to assess the investment of law enforcement authorities in addressing the issues of counterfeiting and piracy online. However, we believe, just as in the offline environment, that law enforcement authorities have a role to play to assist rights holders in enforcing their rights when and where needed.