

Brussels, 22nd September 2010

DIGITALEUROPE RESPONSE TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY IN EUROPE¹

MANAGEMENT SUMMARY

DIGITALEUROPE welcomes the European Commission's initiative on the open Internet and net neutrality in Europe. As the voice representing the Digital Technology in Europe, we are strategically well positioned to comment on this public consultation.

First, DIGITALEUROPE is not aware of any difficulties related to network management practices. We believe the vast majority of concerns raised in the context of net neutrality are purely theoretical and have not manifested themselves in the marketplace. Industry information suggests markets are sufficiently competitive to deter any harmful conduct.

Further, DIGITALEUROPE is of the view that in the event of any potentially harmful conduct, the revised EU Telecoms Framework is appropriately well-suited to respond to the question of the openness of the Internet.

DIGITALEUROPE members have reservations about any proposals which may narrowly define which network management practices are acceptable and which ones are not. In our view, it is important that broadband providers retain broad discretion to employ necessary network management techniques, and the ability to develop and offer innovative new managed services to customers who value these products.

GENERAL REMARKS

DIGITALEUROPE fully supports an open and innovative Internet. As the Commission states in its consultation document, the Internet has never been more central to people's lives than today. Clearly many of the Internet's benefits come from its open nature and the ability of anyone to develop new and innovative devices and services that connect to it. Such innovation has created entirely new industries and has fostered competitive markets in Internet applications and equipment.

¹ Consultation launched by the European Commission on 30 June 2010. The questionnaire is available at http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/index_en.htm.

DIGITALEUROPE therefore fully supports the connectivity principles which are now embedded in the revised Framework Directive, which establishes that national regulatory authorities shall promote the interests of the citizens by, inter alia, promoting the ability of end-users to access and distribute information or run applications and services of their choice.²

We also believe an open and competitive Internet must include the ability for network operators to innovate within the network; therefore it must permit network management and managed services to offer consumers additional choice through tiering, quality of service, security services, and other network management techniques.

In DIGITALEUROPE's view, the ultimate goal from a policy maker point of view should be to maintain an open Internet and permit networks to be adaptively managed to optimise the needs of different subscribers and applications without jeopardising consumer protection or competition.

QUESTION 1: IS THERE CURRENTLY A PROBLEM OF NET NEUTRALITY AND THE OPENNESS OF THE INTERNET IN EUROPE? IF SO, ILLUSTRATE WITH CONCRETE EXAMPLES. WHERE ARE THE BOTTLENECKS, IF ANY? IS THE PROBLEM SUCH THAT IT CANNOT BE SOLVED BY THE EXISTING DEGREE OF COMPETITION IN FIXED AND MOBILE ACCESS MARKETS?

QUESTION 3: IS THE REGULATORY FRAMEWORK CAPABLE OF DEALING WITH THE ISSUES IDENTIFIED, INCLUDING IN RELATION TO MONITORING/ASSESSMENT AND SUBSEQUENT ENFORCEMENT?

[Joint answer to questions 1 and 3 follow]

In regards to question 1 which asks whether there are problems on net neutrality and the openness of the Internet in Europe, we are not aware of any difficulties related to network management practices. We believe the vast majority of concerns raised in the context of net neutrality are purely theoretical and have not manifested in the marketplace.

We view markets as sufficiently competitive and intrinsically enabled to deter harmful conduct. Service providers are disciplined by the competitive market, and the need to retain and add customers by responding to consumer demand.

In response to question 3, in the hypothetical case that market forces would not be sufficient to address harmful conduct, we believe we have adequate tools within the competition and sector-specific framework to safeguard an open Internet, protecting consumers and competition.

In contrast with other jurisdictions, the European Regulatory Framework provides Regulators a direct authority over the provision of electronic communications services, including broadband services. In the context of the new Directives, as outlined by the Commission in its consultation document, there are also specific provisions that have been agreed in order to ensure an open Internet. In addition to the connectivity principles, new transparency rules

² Article 8g Revised Framework Directive

have been adopted, to ensure consumers are aware of any limitations in their broadband service plans. To conclude, a new reserved power is granted to all Regulators in order to impose minimum quality of services to prevent degradation or slowing of traffic over networks.

All these tools enable Regulators to intervene and address potential inappropriate behaviour.

In response to the Commission's remark that *"a number of cases have emerged involving the differentiated treatment by network operators of services or traffic which have led some interested parties to question whether the principle of the openness or neutrality of the Internet may be at risk"*, we would like to remark that differentiated arrangements are common place in competitive sectors throughout the economy and are generally pro-competitive.

The Directives have explicitly moved away from a pure non-discrimination rule, which in our view would inhibit innovation and the ability of providers to adapt to fast changing markets and evolving consumer needs.

We agree a discriminatory behaviour that restricts competition should not be allowed, but there are many examples of "discrimination" or "differentiation" taking place today that are essential to proper functioning of the Internet.

As we explain in more detail in our response to question 4, each network operator employs management tools for a variety of reasons, and may prioritise traffic on networks and may therefore 'discriminate' among the various bits that make up typical Internet traffic. But this form of discrimination is essential to the proper Internet traffic management and a response to ever-changing traffic patterns and other developments.

QUESTION 4: TO WHAT EXTENT IS TRAFFIC MANAGEMENT NECESSARY FROM AN OPERATOR'S POINT OF VIEW? HOW IS IT CARRIED OUT IN PRACTICE? WHAT TECHNOLOGIES ARE USED TO CARRY OUT SUCH TRAFFIC MANAGEMENT?

There are many valid and pro-competitive reasons why a broadband Internet access provider might wish to "manage" traffic on its network: To maintain network security, controlling the proliferation of spam, spyware, worms, and other "malware"; to provide parents appropriate discretion over the content accessed by children; to hamper the unlawful dissemination of intellectual property; and – perhaps most significantly – to ensure quality of service is maintained as the demands placed on the Internet skyrocket.

Indeed, Internet usage is increasingly driven by high-bandwidth applications including, online gaming, video over IP, voice over IP, and peer-to-peer ("P2P") file exchange services. Management tools allow service providers to manage congestion on their networks to ensure that packets associated with latency and jitter sensitive applications arrive on time, and that the end user's experience is not disrupted by network congestion. Without these technologies, consumers will experience more traffic congestion in general and will subject applications (such as video) that require constant quality of service to the vagaries of the public Internet.

There are four major types of network management which we briefly summarise these below:

- (1) **Specialized IP Routing:** Internet service providers (“ISPs”) rely on routing technologies to allow them to adhere to service level agreement guarantees in the face of network congestion and quality of service requirements. IP routing creates a virtual path that data will follow as it moves across a network or networks to its ultimate destination. Explained in simple terms, within the network data is directed using the destination IP address in the packet header according to forwarding tables used by routers. These are based on a series of protocols. By employing IP routing that responds to prevailing traffic demands, broadband providers engineer traffic patterns to improve performance. IP routing technology innovations include multi-protocol label switching (“MPLS”) a data-carrying mechanism by which data packets are assigned labels and forwarding decisions are made solely on the basis of these labels - without the need to examine the packets themselves. As a result, virtual links can be created between distant nodes using any protocol, further enhancing reliability of the network.
- (2) **Packet Differentiation (using so called “DiffServ model”):** Originally envisioned by the Internet Engineering Task Force, the DiffServ model allows for IP quality of service distinctions to be applied to various groupings of network traffic. Data will be classified into different classes of network traffic, which will define how that network traffic is forwarded as it flows across different routers in the network. Data traffic may be further conditioned by tools such as metering, marking, policing and shaping in order to adhere to service level guarantees or to address network challenges. These traffic tools can be used to reduce load peaks and queuing delays and to assure that the priority traffic goes out first. For instance, in a network that is subject to congestive collapse, traffic conditioning can be used by an ISP to ensure that the packets associated with an emergency government communication are transmitted with a minimum of loss or jitter.
- (3) **Filtering:** ISPs may employ traffic filtering in order to enhance network security. Traffic filtering is a technique used to enforce access control policies in order to ensure network security and quality of service. By way of example, a network access control list can be used as a traffic filtering tool by an ISP to control inbound and outbound traffic. Such lists and more complicated filters allow an ISP to distinguish between traffic that is “safe” and traffic that is “harmful.” If ISPs were deprived of the ability to filter their traffic, their options for responding to a network attack would be severely limited.
- (4) **Caching:** Some content providers and broadband networks operators have developed content distribution methods that would involve direct interconnection and caching of content not just *close to* the broadband provider’s access/aggregation networks, but *within* those networks as well. This enables end users to gain access to that content with shorter latency and reliably. It brings the customers the quality of experience he chooses for the content he wants. This will be essential for the management of the data explosion.

QUESTION 5: TO WHAT EXTENT WILL NET NEUTRALITY CONCERNS BE ALLAYED BY THE PROVISION OF TRANSPARENT INFORMATION TO END

USERS, WHICH DISTINGUISHES BETWEEN MANAGED SERVICES ON THE ONE HAND AND SERVICES OFFERING ACCESS TO THE PUBLIC INTERNET ON A 'BEST EFFORTS' BASIS, ON THE OTHER?

Europe benefits from a vital and dynamic status of competition at retail level. DIGITALEUROPE members know from experience that competition, together with transparency provisions is perfectly able to allay net neutrality concerns. In a competitive environment an obligation to transparency ensures that consumers are provided with the means to make well informed decisions. We are of the opinion that the revised EU Telecoms Framework is very well-suited to respond to the question of the openness of the Internet. Given that transparency obligations are incorporated into the package, network management and quality of service differentiation necessary for an optimised user-experience involving time and resource critical traffic can be tackled. Reliability of network and service delivery, network and service performance as well as congestion-handling need to go hand-in-hand with providing the user with all the information necessary to make educated decisions in regards to choosing the right packages to fulfil their requirements.

Information to the consumer should contain easy to understand descriptions of traffic management practices that are applied and how these practices can influence the end User's experience. DIGITALEUROPE believes that guidance by national regulators at such early stage of the debate is helpful in order to make different offers comparable.

QUESTION 6: SHOULD THE PRINCIPLES GOVERNING TRAFFIC MANAGEMENT BE THE SAME FOR FIXED AND MOBILE NETWORKS?

Traffic management is a function which is essential whenever the capacity demand exceeds the available network capacity at any given point. To this end, it is an essential network management function.

Telecommunications networks are planned and deployed along certain parameters (e.g. max data capacity, call drop rates, end-to-end latencies etc) to satisfy envisaged end-user requirements. According to e.g. business expectations, these parameters may be different for various (competing) telecom providers (operators) and include assumptions about future service developments and network technology evolution, where possible. In addition, mobile networks require distinct radio network planning to guarantee service coverage at a suggested quality level (e.g. 90% time and place).

Today, mobile and fixed telecommunication infrastructures are based on different network topologies for offering Internet access to end users:

- Fixed networks operate on a variety of network topologies including both dedicated and shared access medium for the final stage of the link to each user's premises. Examples of dedicated access on the final stage include cases where each user has e.g. a dedicated fiber optic (in case of FTTH) or copper cable (in case of xDSL) coming to his home for his own access to the network. Examples of shared access include structures where the common resource is shared amongst a number of subscribers (e.g. PON, cable networks applying DOCSIS). Traffic management procedures and measures need to ensure fair access for multiple Users, if the instant

resource demand of all users at any point of concentration is higher than the entire carrier capacity supported.

- Mobile networks are centered on a shared resource (the radio network and interface, amongst others governed by the amount of spectrum used) to provide 'last-mile' access to the network for all users within a given mobile cell. In addition, users in a mobile network are inherently changing their locations and, hence, cell affiliations which results in rather dynamic traffic demand. Therefore, traffic management is an inevitable function to guarantee proper and stable operation, since one user's behaviour could influence another user's quality of service. This happens whenever several users are requesting more resources than available from a single infrastructure access point. If this situation occurs over a longer period, the radio cell is said to be congested. In reality, the radio resource control of the system will deal with this. However, it needs to have knowledge about proposed strategies in order to do so.

In summary, the traffic in mobile networks has to be managed in order to mitigate the effects of congestion, in a spectrum efficient way³. This could be done pre-emptively or on-demand at the time when it occurs.

Usually, once the access bottlenecks have been overcome (sharing of resources across users) fixed networks can implement less stringent management procedure to supply user quality of service, most frequently being done by so-called over-provisioning of resources.

One clear example of traffic management is that emergency calls over mobile network will be given priority over other traffic in order to ensure that calls of this nature can always be made, even in situations of peak demand, such as inside a stadium during a large scale event.

Traffic management has to follow certain rules which are determined through network management procedures. This could include prioritising certain services over others according to their QoS demand parameters (such as delay, speed, service level agreements etc) as well as user demand in view of their tariff models. To this end, traffic management is a generic function applicable to managing the service of both fixed and mobile networks and must work inside the boundaries of the service level agreement agreed with the end-user.

While the principles of traffic management could be the same for both fixed and mobile networks, the measures will differ.

Mobile and fixed network operators are likely, amongst others, to apply the following policy principles which are outlined below as an example for mobile networks:

³ Some business strategies can be implemented to limit the risk of congestion due to high consumptions (e.g. video streaming) within a mobile cell: for instance broadcasting most watched video programmes over broadcast links (one transmission link, with virtually unlimited number of receiving users within coverage area) either in real time (as TV) or in distribution push mode (receive, store, and retrieve later most watched video clips) are well understood techniques to offload video traffic away from mobile networks, and decongest them for genuinely interactive communication

- **Quality of Service and network management:** Advanced traffic management techniques and radio access optimisation is indispensable to ensure the best use of limited spectrum capacity for the benefit of all users and to stabilise network operation: to mitigate congestion, ensure quality of services increase network stability and to offer mobile broadband services at various service quality levels, as demanded by users.
- **Bandwidth efficiency of applications:** Applications in Internet are often developed without taking into account the amount of traffic they generate. In effect, in an environment of very high speed fixed access such as FTTH, there is no incentive for developers to optimise the bandwidth requirement of their application, as well as no awareness from the consumer about the resulting traffic. However, as the bandwidth, is constrained in mobile broadband networks, bandwidth efficient applications should be promoted towards consumers and developers in order to avoid wasting finite resources.
- **Innovation and new business models:** Operators should be able to apply any suitable business models regardless of the type of infrastructure. Competition as well as technology and service innovation through new business models should neither be constrained nor limited. Effective competition across the Internet value chain and the emergence of new business models, as already initiated in mobile broadband with “sponsored connectivity” or payment per-transaction⁴ are important for the generation of new revenue streams among the various stakeholders, and positively contribute to the willingness to invest in new network functions and capabilities – to extend service variety, network coverage and traffic capacity. This may include off-loading of data-intensive (indoor) traffic onto fixed networks (e.g. using Wi-Fi access or Femtocells).

In conclusion, it is our view that basic principles of traffic management do not necessarily depend on the network type, in contrast they could be very much the same, but the mechanisms will differ. The target of traffic management is purely to protect the network from overloading and, hence, to assign network resources on the basis of traffic demand and designated rules.

QUESTION 7: WHAT OTHER FORMS OF PRIORITISATION ARE TAKING PLACE? DO CONTENT AND APPLICATION PROVIDERS ALSO TRY TO PRIORITISE THEIR SERVICES? IF SO, HOW – AND HOW DOES THIS PRIORITISATION AFFECT OTHER PLAYERS IN THE VALUE CHAIN?

No response can be offered at this time.

⁴ “Kindle model” whereby Amazon pays the mobile operator for connectivity and the users pay directly to Amazon for the content (books) which get downloaded over the operator network. Other examples include connected Personal Navigation Services (“TomTom Live Services”), connected Digital Photo Frame (“Pandigital Photo Mail”), child/family tracker (“LittleBuddy”)

QUESTION 8: IN THE CASE OF MANAGED SERVICES, SHOULD THE SAME QUALITY OF SERVICE CONDITIONS AND PARAMETERS BE AVAILABLE TO ALL CONTENT/APPLICATION/ONLINE SERVICE PROVIDERS WHICH ARE IN THE SAME SITUATION? MAY EXCLUSIVE AGREEMENTS BETWEEN NETWORK OPERATORS AND CONTENT/APPLICATION/ONLINE SERVICE PROVIDERS CREATE PROBLEMS FOR ACHIEVING THAT OBJECTIVE?

It is expected that competition will result in service providers and consumers being able to access the full range of QoS offers. However, if it can be concluded that the market failed to meet consumer needs regulatory measures, as per the intentions of the telecom package, may need to be considered. If a market participant chooses not to accept a QoS offering from an operator, preferring instead a best efforts offer, which results in different quality of service conditions, this is not the responsibility of the operator. The requirement to provide equivalent offers to different players should guard against discrimination between applications and services on the operators own commercial grounds. Under these conditions end user demand will ensure solutions that offer consumers greatest value propositions are successful.

Exclusive content agreements should be permitted, particularly given a) there exist multiple platforms for disseminating content and b) competition law applies in any case.

End-to end service offerings must be secured in order to protect an open Internet; such end-to-end guarantees would be part of the 'best efforts' obligations of an operator.

QUESTION 9: IF THE OBJECTIVE REFERRED TO IN QUESTION 8 IS RETAINED, ARE ADDITIONAL MEASURES NEEDED TO ACHIEVE IT? IF SO, SHOULD SUCH MEASURES HAVE A VOLUNTARY NATURE (SUCH AS, FOR EXAMPLE, AN INDUSTRY CODE OF CONDUCT) OR A REGULATORY ONE?

Existing rules give national regulators the power to intervene should discrimination occur. The European Commission and BEREC could assist National Regulatory Authorities by clarifying what qualities a 'best efforts' package contains. Given political concerns that new premium quality of service offerings could lead to a degrading of 'best efforts' service policymakers would be well served to define 'acceptable efforts' quality levels such that this is clear to network operators and can be consistently applied across the European Union by the different NRAs. This would avoid uncertainty for network operators, regulators and consumers.

The European Commission and BEREC, jointly with NRAs, should also monitor that transparency obligations are being met.

In addition, acceptable quality of service depends on the nature of a user's application and service use and is something that will change over time. Where some users may have a 24mb connection and be unhappy with the QoS, other may have 1mb and be content. Such judgements are thus subjective as well as objective. They will also keep changing as broadband speeds increase, as application and online services become more bandwidth intensive or sensitive to other network measures such as latency. Consultations with network user groups (content service providers and consumers) about satisfaction with 'best

efforts' or 'acceptable efforts' class of performance would therefore be beneficial in helping to understand where guidance is best positioned and how it should change over time.

QUESTION 10: ARE THE COMMERCIAL ARRANGEMENTS THAT CURRENTLY GOVERN THE PROVISION OF ACCESS TO THE INTERNET ADEQUATE, IN ORDER TO ENSURE THAT THE INTERNET REMAINS OPEN AND THAT INFRASTRUCTURE INVESTMENT IS MAINTAINED? IF NOT, HOW SHOULD THEY CHANGE?

The challenges and the future development of the Internet should be taken into account. Investment in ubiquitous access (wireless and wireline) is enormous, and up-grades in the core and backhaul of the networks will also be required to cope with explosion of traffic data we are seeing in the Internet, and the development of new services and applications, which will continue to grow. The Internet of today and of tomorrow will continue to see the emergence of multiple actors that requires seeing it as a two sided (or multi-sided) market.

Today the Internet interconnect market is competitive and functions well based on commercial negotiations. Nevertheless, we support the need for Regulators to continue to closely monitor the evolution of this complex eco-system.

The current framework is based on the principle of free negotiation of interconnection agreements (Article 3 (a) Access Directive) and on the theory that competition and the application of competition law are sufficient, unless there is evidence to the contrary to correct malfunctions or abuse by players. We do not think there any evidence today to suggest there is a requirement for ex-ante intervention in this market. There is an evolution of the Internet interconnection models taking place and we will also see the emergence of new business models for the broadband Internet. For example, it is not entirely clear that the single-sided, "subscriber pays a flat rate" model is always in the best interests of consumers, and new types of models are being tested which can reduce the cost to consumers, increase consumption of communication service and benefit all parties.

Regulators should be careful not to intervene to favour one particular set of actors in what should be a commercial legitimate negotiation, unless there is an identifiable market failure or abuse of dominant position.

QUESTION 11: WHAT INSTANCES COULD TRIGGER INTERVENTION BY NATIONAL REGULATORY AUTHORITIES IN SETTING MINIMUM QUALITY OF SERVICE REQUIREMENTS ON AN UNDERTAKING OR UNDERTAKINGS PROVIDING PUBLIC COMMUNICATIONS SERVICES?

The answer to this question is lack of voluntary minimum QoS commitment and lack of communication to the consumers. For internal market and e-Inclusion reasons a basic best effort Internet offering should be uniform across the EU.

With regard to question 11 and the implementation of the reserved power foreseen in article 22.1, there may be a need to clarify how these powers, if necessary, can be exercised. This could be done by the Commission, through guidelines to Regulators, or at the BEREC level. We would have reservations about any proposals that may narrowly define which

management practices are acceptable and which ones are not, beyond general provisions to avoid blocking or degradation in an anti-competitive way. We would also be concerned with a pure non-discrimination requirement, for reasons already explained.

In our view, it is important that broadband providers should retain broad discretion to employ necessary network management techniques, and the ability to develop and offer innovative new managed services to customers who value these products. Likewise, as explained in question 10, it is important that providers retain the ability to engage in two-sided or multi-sided business models, involving service providers, application or content providers, and consumers. These types of arrangements can be both more efficient and equitable, and reduce broadband costs for consumers and increase adoption.

QUESTION 12: HOW SHOULD QUALITY OF SERVICE REQUIREMENTS BE DETERMINED, AND HOW COULD THEY BE MONITORED?

Transparency about the quality/performance parameters for a broadband connection is essential to the consumer,. Performance criteria for such networks can be measured by throughput and delay statistics. That means the proportion of traffic is in-line with a certain delay time (milliseconds) and a certain data throughput (Mbps) .

QUESTION 13: IN THE CASE WHERE NRAS FIND IT NECESSARY TO INTERVENE TO IMPOSE MINIMUM QUALITY OF SERVICE REQUIREMENTS, WHAT FORM SHOULD THEY TAKE, AND TO WHAT EXTENT SHOULD THERE BE CO-OPERATION BETWEEN NRAS TO ARRIVE AT A COMMON APPROACH?

See answers to questions 11 and 12 above.

QUESTION 14: WHAT SHOULD TRANSPARENCY FOR CONSUMERS CONSIST OF? SHOULD THE STANDARDS CURRENTLY APPLIED BE FURTHER IMPROVED?

DIGITALEUROPE supports an open Internet where users can access content and services of their choice. The openness of the Internet as such has been its groundbreaking principle and basic strength enabling everybody to participate. Having said that only an informed user has the capability to decide which services he or she wants to use. In order to make an informed decision, transparency regarding availability and access of services and content is a prerequisite.

DIGITALEUROPE is of the opinion that the provisions in the Universal Service Directive are sufficient to address transparency requirements. In particular Art 20 (b) which gives end users the right to “information on any procedures put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures could impact on service quality,” together with Art 21 (3) d which gives national regulatory authorities the possibility to oblige undertakings providing public electronic communications networks and/or publicly available electronic communications services to “provide information on any procedures put in place by the provider to measure

and shape traffic so as to avoid filling or overfilling a network link, and on how those procedures could impact on service quality” provide a clear legal basis for transparency.

As the Universal Service Directive gives Member States in Art 22 (3) also the possibility to enable national regulatory authorities to set minimum quality of service requirements in order to prevent the degradation of service and the hindering or slowing down of traffic over networks, DIGITALEUROPE is of the view that the legal basis for transparency requirements is granted.

QUESTION 15: BESIDES THE TRAFFIC MANAGEMENT ISSUES DISCUSSED ABOVE, ARE THERE ANY OTHER CONCERNS AFFECTING FREEDOM OF EXPRESSION, MEDIA PLURALISM AND CULTURAL DIVERSITY ON THE INTERNET? IF SO, WHAT FURTHER MEASURES WOULD BE NEEDED TO SAFEGUARD THOSE VALUES?

The online services that have been developed since the advent of the Internet have blossomed since the Directive on Electronic Commerce was one of the EU’s early information society Directives and forms one of the most important foundations on which online businesses in Europe are built. Amongst other matters, the directive deals with the liability of intermediaries. The delicate balance struck in that debate provides the cornerstone of the Internet economy and society by laying down the rules for what online intermediaries are and are not liable for. This has served as the basis for much online trade and, equally importantly, channels of online expression, new forms of media and for diverse communities.

Imperative for a vibrant ecosystem for the web services ecosystem is the maintenance of the existing liability rules and their consistent application across the EU. The rules strike a careful balance between the interests of different parties. However, some stakeholders do not consider the role of liability rules in a comprehensive way and therefore fail to appreciate the side-effects (e.g. for freedom of expression) of changes to this delicate balance.

It is therefore important that the European Institutions avoid unnecessary changes to this regime in order to preserve online freedoms and to provide legal certainty to online businesses.

ABOUT DIGITALEUROPE

DIGITALEUROPE is the pre-eminent advocacy group of the European digital economy acting on behalf of the information technology, consumer electronics and telecommunications sectors. We are dedicated to improving the business environment, and to promoting industry's contribution to economic growth and social progress in the European Union.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 63 leading corporations and 40 national trade associations from all the Member States of EU; altogether 10,000 companies with 2 million employees and €1,000 billion in revenues. You can learn more about our activities via <http://www.digitaleurope.org>

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Adobe, Agilent, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, Bose, Brother, Buffalo, Canon, Cassidian, Cisco, Corning, Dassault Systems, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, IBM, Ingram Micro, Intel, JVC, Kenwood, Kodak, Konica Minolta, Lexmark, LG, Loewe, Micronas, Microsoft, Mitsubishi, Motorola, NEC, Nokia, Nokia Siemens Networks, Nortel, NXP, Océ, Oki, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, Sanyo, SAP, Sharp, Siemens, Sony, Sony Ericsson, STMicroelectronics, Technicolor, Texas Instruments, Thales, Toshiba, Xerox.

NATIONAL TRADE ASSOCIATIONS:

Austria: FEEL; **Belgium:** AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Czech Republic:** ASE, SPIS; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** ALLIANCE TICS, SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy:** ANITEC; **Lithuania:** INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE, APDC; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AETIC, ASIMELEC; **Sweden:** IT&TELEKOMFÖRETAGEN; **United Kingdom:** INTELLECT; **Belarus:** INFOPARK; **Norway:** ABELIA, IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE