

A Fair Internet for All
Strengthening Our Citizens' Rights and Securing a Fair Business Environment
in the Internet

EPP Group Strategy Paper

I. Mandate of the Working Group

The EPP Working Group "Internet Today and Tomorrow" was set up by decision of the Group Presidency on 11 May 2010. The intention of the Presidency was to elaborate an EPP Group strategy with regard to the Group's Internet policy in order to tackle the different questions that were raised by members due to current problems. Instead of addressing these in a piece-meal approach, the Working Group was founded in order to prepare a coherent EPP Group strategy.

The Working Group is chaired by MEP Angelika Niebler. Deputy Chairman is MEP Philippe Juvin. The Group held nine meetings¹ under the following broad headings: (1) Business philosophy in the Internet, covering issues such as search neutrality, net neutrality, online advertising, intellectual property rights as well as quality of online journalism; (2) private user's expectations addressing data protection issues related to social networks, cloud computing, profiling and privacy; and (3) matters of public interest, discussing, for example, the protection of minors online. Overall, a broad variety of issues were covered in order to give a comprehensive recommendation to the Group with regard to its future position on these questions.

II. The Internet of tomorrow: The Need for Political Debate

The Internet is a multi-faceted economic and social space. Its extremely fast development has created a new world of possibilities, challenges as well as risks for businesses, citizens and states. It is an exceptional platform for innovation, economic growth and social communication. By means of the Internet, entrepreneurs reach global markets, political groups debate, communicate and organise, and major companies manage their supply chains and deliver services to their customers. Simply stated, the Internet has become the central nervous system of our information economy and society.

Over the last 15 years, personal computers, mobile phones and other devices have transformed how we access and use information. As powerful, exciting and ground-breaking as these developments are, they also raise new concerns. New kinds of devices and applications allow for the collection and use of personal information in manners that, at times, can be adverse to users' privacy expectations. Also, the world has witnessed a growing collection of cyber security threats and struggles to keep emerging vulnerabilities in check.

Approaching these and other issues in a manner that preserves the extraordinary economic and social potential and the freedom of the Internet without impeding innovation requires a fresh look at our Internet strategy. Guaranteeing freedom of expression, free flow of information and access for everyone as well as taking care of individual rights and business needs remain the cornerstones of our approach.

¹ Meeting of 17 June 2010 - "Brainstorming Meeting", meeting of 8 July 2010 - "Business Philosophy in the Internet", meeting of 09 September 2010 - "Private User's Expectations", meeting of 7 October 2010 - "Intellectual Property Rights in the Internet", meeting of 25 November 2010 - "Net Neutrality", meeting of 16 December 2010 - "Social Internet", meeting of 20 January 2011 - "Quality Journalism Online", meeting of 17 February 2011 - "Cloud Computing", meeting of 7 April 2011 - Open discussion

1. Business Philosophy in the Internet

(a) Creating more competition by strengthening the European pillar of the Internet

Much has been achieved in recent years at EU level in order to make Europe a truly knowledge-based economy. Not only the domain ".eu" has been a success but more importantly the EU2020 Strategy has dedicated one of its flagship initiatives to this end, the so-called New Digital Agenda for Europe.

Nevertheless, the European economy is still lagging behind its major competitors, notably the US, due to, inter alia, its failure to develop IT skills, innovation and research and development (R&D). The EU therefore has to develop the necessary political vision and policies to remain competitive. It must deliver on the knowledge-based economy, create a business-friendly online surrounding and establish a level playing field by obliging Internet service providers (ISP) to comply with the same EU standards with respect to data protection, data privacy and consumer protection as well as IPR protection. It is furthermore necessary to increase investments in R&D in order to enhance EU capacities and to keep up with the pace of high-tech developments and innovations.

(b) Search Neutrality

Nowadays search engines have taken on the role of the Internet's gatekeepers due to their ability to direct users to websites. By basing their search on algorithms which highlight some information, privilege some websites and fail to include others altogether they determine the information which users access online. In this way, they can deter market entry in areas which could benefit consumers and harm possible entrants.

This is particularly the case when search engines not only offer search services but use their platforms for distributing their own products or services. Therefore, there is a need to have a careful eye, in particular, on the interlinking of services. Interlinking does not necessarily constitute anti-competitive behaviour but there is large potential for abuse, such as lowering the ranking of unpaid search results of competing services and giving preferential placement to the results of own products.

This abuse has to be prevented in order to keep the Internet business-friendly allowing for more choice and more competition. The Commission needs to closely investigate the potential abuse of a search engine's dominant market position.

However, from the users' perspective, information about the underlying rules (not algorithms) governing indexing, searching and prioritising, should be fully and truthfully disclosed in a way that is meaningful to the majority of web-users. The disclosure should also cover agreements between the search engines and third parties influencing the choice of websites. Of course, it needs to be stressed that the search neutrality debate should not be about making search algorithms public. These are search engines' intellectual property and thus deserve full protection. Disclosing search algorithms would only benefit spammers and would lead to search results being dominated by spam.

(c) Net Neutrality

The EPP Group understands net neutrality as the guiding principle which preserves the neutral transmission of data, regardless of its content, origin and application which created it. As such, the EPP Group enshrines net neutrality as a policy objective that needs to be implemented at EU level. It is of crucial importance to provide a level playing field for all actors in the web. As such, it is a fundamental characteristic of the free and open Internet.

The full realisation of net neutrality is yet challenged everyday due to an increasing amount of data transmitted online. This requires a permanent rise in capacities and thus investment by telecom

providers. Especially new services, such as IPTV (Internet protocol television), video on demand, streaming services as well as the growing use of smart phones, create more data traffic. If the amount of data exceeds router capacity, delays, latencies or losses follow.

However, the European Commission's report on net neutrality of April 2011 proves that practices of unequal treatment persist.² The results of a 2010 survey conducted by BEREC (Body of European Regulators for Electronic Communications) in several EU Member States show that limits were set on the speed of peer-to-peer file-sharing or video streaming by certain providers in France, Greece, Hungary, Lithuania, Poland and the United Kingdom. In addition, certain mobile operators in Austria, Germany, Italy, the Netherlands, Portugal and Romania blocked or charged extra for the provision of voice over internet protocol services in mobile networks.³

Such discriminatory practises cannot be tolerated. Accordingly, the EU regulatory framework for electronic communication forbids any access differentiation based on content or any discriminatory procedures with regard to access for new services. This is also in the interest of the users.

However, from a user perspective, it is acceptable that data services or applications are transmitted to users according to different speed and data amounts. A "pay-for-priorisation-system", for instance, allows consumers to choose between several service delivery speeds (quick and more expensive versus slower and cheaper) and/or data volumes. To this end, it is important that the user, instead of the ISP, chooses the speed and volumes of downloads and services.

Another issue is that ISPs often do not provide consumers with the actual speeds of their connection versus the advertised speeds. ISPs should only be allowed to advertise with the minimum speed they can provide for, not the maximum speed. The ban on misleading advertising must therefore be coherently enforced.

2. Private Users Expectations

Private users' expectations focus on an open Internet which is easily accessible and where European standards for data protection are respected. As the legal framework for data protection is currently under revision, some cornerstones should be laid down for the political debate.

(a) Jurisdiction and Oversight

According to Article 8 of the Charter of Fundamental Rights of the European Union, data protection is a fundamental right. The situation is however different in many third countries where data protection is widely acknowledged but not granted the same status or where enforcement systems differ fundamentally.⁴

The EU and its Member States must ensure that data protection is guaranteed for all EU citizens also in the context of a globalised world. To counterbalance the risks and dangers resulting from new technological developments, the data protection framework must be fully harmonised according to a very high level of protection within the EU as the Internet is equally open to all EU citizens. This full harmonisation will ensure legal certainty, reduce administrative burdens as well as economic costs and avoid the risk of "forum shopping" between more or less stringent national legislations.

² European Commission, 19 April 2011, "The open internet and net neutrality in Europe", http://ec.europa.eu/information_society/policy/ecomms/doc/library/communications_reports/netneutrality/comm-19042011.pdf

³ BEREC, "BEREC's response to the European Commission's consultation on the open Internet and net neutrality in Europe", September 2010, http://erg.eu.int/doc/berec/bor_10_42.pdf

⁴ For more details on the EPP position on the revision of the Data Protection Directive see: [Title of the EPP position paper and electronic reference].

Furthermore, EU standards must apply to all data collected within the EU, even if these data are stored outside the borders of the EU. This means that individuals must have the right to claim protection also if their data are processed outside the EU.

In addition, it is crucial that the principles and elements set out in Directive 95/46/EC are fully implemented and applied in the online environment as they are offline since they are not only sound but also technologically neutral. These include the principle of transparency, data minimisation and purpose limitation as well as the provisions of consent.

Moreover, "privacy by design" and "privacy by default" need to be explicitly included as general binding principles into the existing data protection legal framework. In addition, the accountability principle must be incorporated pursuant to which data controllers are obliged to carry out the necessary measures to guarantee that the principles and obligations of data protection law are adhered to. This compels their implementation by data controllers and ICT designers and manufacturers while offering more legitimacy to enforcement authorities to require effective implementation in practice.

One of the existing pillars of an international system, the Safe Harbour Agreement with the US, is in urgent need to be re-revised as it seems to create an imbalance in data protection obligations for EU enterprises and US-based enterprises. This agreement is in fact aiming at ensuring that US commercial providers protect data of EU citizens in the same way as within the EU, however, the control mechanisms do not seem to be efficient enough to achieve this. Therefore, either the deplorable deficits in the implementation of the agreement will be solved quickly or the agreement has to be dissolved.

(b) Social Networks

Social networks are not only mere platforms where users can enter into communication and share information: they also bring people together, create new interpersonal relationships thereby having a cultural and societal dimension. In particular, young people recklessly disclose personal information in social networks and post photographs carelessly to all their social network friends.

As fascinating as this new opportunity of communication is, these networks also raise a number of questions with regard to the creation of an identity in the net without any evidence, privacy controls, protection of minors, and data ownership.

Based on the personal information users disclose online, in combination with data tracing users' actions and interactions with other users, an informative profile of that person's interests and activities can be created. This can then be used by third parties for a variety of purposes, such as commercial purposes, and may pose major risks such as identity theft, financial loss, and physical or mental harm.

Social networks must inform users about the purpose and different ways in which they intend to process members' data. A link to this information should be visibly incorporated onto each social network's website. This information must explain in an easily understandable way what kind of data is being processed, for what purpose, what kind of tools are used, and if it is transferred to third parties. Social networks must be obliged to incorporate privacy-friendly default settings. Each new account registration should implement the highest security standards from the beginning which can then be lowered by the user. A complaint facility should be made obligatory for every social network site to serve members in case of data protection issues.

Since users and not platforms or networks are the owners of personal information they must be in full control of the information, data and images they provide, including the right to delete this information. The currently discussed "right to be forgotten" and the establishment of "digital erasers" are promising, however, there is still need for clarification of what exactly this right entails, who is affected by it and how it is technically feasible.

More efforts must be made by both social networks and the Commission to educate citizens about privacy risks. Social networks must provide adequate warnings to members about privacy risks and data protection rights when uploading information online. Given that the general public is often unaware of issues surrounding the use of personal data and the tools available for addressing them, information campaigns must be launched and education material be produced to inform Internet users about the technologies available to manage traces left in the web, and on how to protect their privacy.

(c) Online Behavioural Advertising

Behavioural online advertising involves the observation of users' online activity by collecting information about when they access the web and what websites they visit. Based on this information advertising network providers can create profiles over time in order to provide users with advertisements matching their interests.

Online advertisers use different techniques to deliver behavioural advertising. On the one hand, there is data crawling to describe the collection of personal data by searching publicly accessible websites. The basis of this is a tool which collects information about contacts on the net, e.g. which websites were opened and which e-mail addresses were contacted. On the other hand, there is data profiling meaning the combination of personal data coming from various sources. Until now, most providers deny that they use data profiling, however, data protection supervisors have no access to verify these statements.

First and foremost, all actors engaged in online behavioural advertising need to comply with the provisions of the EU data protection framework. The new data protection legal framework must ensure that practices of data profiling are forbidden. Furthermore, the new data protection framework should oblige commercial actors to inform consumers about practices associated with behavioural advertising in a transparent way. This information should be displayed directly and visibly on the screen."

Advertising technologies utilise cookies as a means to analyse users' online activity. In principle, cookies are no threat to the security of the net or individual device; however, abuse is always possible. Hence, there is a need for the revised EU data protection framework to establish rules for the use of cookies, e.g. the automatic deletion after leaving a website, except if the consumer accepts the preservation of cookie for further use

(d) Anonymity of the User

New services, e.g. analytic services, allow the owner of a website to get detailed statistics on the visitors of their website and provide them with an analysis of the activities of the visitor. For these purposes, IP addresses of visitors are analysed and transferred. Regardless of the qualification of the IP-address as personal data, all ISP who dispose of information related to the user allowing them to individualise a person based on an IP address must be subject to the same rules and standards that apply to telecommunication providers. The risk of a violation of data protection is similar, that means that the safeguards must follow the same pattern. This ensures that collection of statistical data will be possible in the future and, at the same time, protects the privacy of the person behind the IP address.

(e) Geolocalisation Services

Geolocalisation services are a new market in development, allowing ISP on the basis of the localisation of the user to provide useful information, e.g. maps, touristic information etc. There are no clear rules for ISP today; on the other hand there are models for regulation, e.g. in the area of mobile telecom providers. Telecom providers are obliged to collect and store localisation data for purposes of prosecution, however, any use of this information is banned and the storage of this information is subject to rigid data protection rules. It needs to be stressed that the collection of location-related data

without request by the user must be forbidden. Thus, legislation must be implemented swiftly; taking into consideration that jurisdiction in these cases is evident as the localisation takes place within the EU.

(f) Cloud Computing

For the EPP Group "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".⁵

All over the world companies increasingly realise the gain of productivity they can achieve by outsourcing through the cloud. It is estimated that by 2014 cloud services revenue will reach USD 148.8 billion and that 60% of all server workload will be virtualised by 2012.⁶

Taking into account the promising economic and commercial prospects of the cloud there is a strong business case for its development. Cloud computing will continue to develop in one or another way and Europe should not take on a passive observer position in this process. It is now the time for Europe to take action and develop a strong and efficient European Cloud Computing Strategy.

When developing a European Cloud we need to take into account the following three conditions that it must fulfil. First of all, the cloud must be technically reliable and resilient. This means that there must be a minimum number of backup positions to prevent the loss of data in case of a harmful event. Secondly, the cloud must be secure. It must provide for a liability scheme and technical standards (e.g. the digital signature), including authorisation and certification schemes. There are technical possibilities to ensure that a cloud is secure against viruses and other cyber attacks, yet, there is a need to oblige providers to make use of the technical possibilities. Thirdly, the cloud must be designed in a way that European users' data are protected according to the EU standards. Data might be secured in one country but not in another. In this respect, Member States governments and the Commission must build on the fact that Europe has been a leader in data protection since 1995 and turn that regime into a competitive advantage for a future market of cloud services. Either EU jurisdiction must be extended to all data collected within the EU or via international agreements which allow the EU to control that its standards are kept in third countries.

Lastly, it must be stressed that when developing a European Cloud, the EU must also tackle enabling factors that might not seem directly related to the cloud but will have an important impact in its development and take-up. It should not be forgotten that strong fixed and mobile communication networks are a prerequisite to grasp the full potential of the cloud. In addition, international jurisdiction will have a huge impact on the cloud. Interoperability and open specifications are essential to have an open and competitive cloud.

⁵ NIST, 2009, "The NIST definition of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

⁶ Gartner, 2009, "Gartner says worldwide cloud service market to surpass \$68 billion in 2010", <http://www.gartner.com/it/page.jsp?id=1389313>;
IDC, 2009, "The economics of virtualization: moving toward an application-based cost model", <http://www.vmware.com/files/pdf/Virtualization-application-based-cost-model-WP-EN.pdf>

3. Securing a Fair Business Environment

The fast development of the internet does not only challenge the traditional views on privacy and consumer protection. The internet has made it possible that new enterprises, developing and using new business models, established themselves on the markets. Taking the boost of some online businesses into account, one must not forget that economic welfare is based on a fair business environment. This means that online business and offline business are bound by the same rules on competition, consumer protection, respect of intellectual property rights and other legal requirement.

(a) Intellectual Property Rights in the Internet

The protection of Intellectual Property Rights (IPR) is one of the pillars of the economic use of the Internet and a prerequisite of the digital economy in the EU. It is also a major challenge for the creative and innovative industries and for the press. The key challenge for the future successful growth of the digital arena, including e-commerce, is to ensure consumer and businesses trust the online environment. For the digital single market to become a reality trust in the digital environment has to be a backbone of this single market.

More and more copyright protected works (music, books, movies, TV shows, games, software, and newspapers) are illegally available on the Internet without the authorisation of the right holders. This does not only have legal implications but IPR infringements also constitute a genuine threat to our economies, societies and cultural diversity.

Trademark law also suffers from certain Internet practices (e.g. sale of registered brand names as advertising keywords in online searches without prior authorisation from the owner of the brand in question). It is essential to ensure that trademarks benefit from the same protection both offline and online.

The development of a single market in the online environment is impeded by the threat that all forms of IPR infringement represent to physical goods (counterfeited and pirated products sold online) and digital works (piracy). In this respect, the question of enforcement of IPR online is of a crucial importance.

On the one hand, according to customs figures, the seizure of infringing items sourced and purchased through the net has increased dramatically all over Europe. On the other hand, as regards music downloads, for every legal download, there are 19 illegal downloads.

Rights holders must be adequately and effectively protected when their works are disseminated online. Several solutions were brought to the discussion: public awareness campaigns, warnings and deterrent measures for repeat infringers and continuous improvement of a legal offer. Since voluntary agreements and dialogues between stakeholders have not lead to any solutions, the EU must adopt a comprehensive legal framework addressing the enforcement of IPR to tackle infringements online. When readjusting this legal framework, the changing quality of ISP must be taken into account and a modification of the liability regime for intermediaries, and their cooperation in IPR protection online, needs to be further explored.

(b) Quality Journalism Online

Practical solutions to balance the interests of digital innovation and quality journalism need to be investigated. There is a clear public interest in preserving neutral and highly qualified journalism as newspapers are still being considered the most reliable source of information. In contrast to most other sources in the net, they allow to clearly identify the origin of an article, its relevance and reliability. The Commission is thus called upon to examine the option of introducing ancillary copyright

provisions which protect content owned by publishers from being used for free by online news services.

Furthermore, many publishers now offering new paid-for on-line solutions are faced with technological giants that may want to control the various dimensions of content distribution. Especially the area of applications is controlled by a limited number of enterprises. This leads to publishers losing some core competencies, such as price setting, as well as their direct relationships with readers via subscription management. Thus, in order to be able to properly adapt to readers' shifting consumption habits, the agents in each phase of the value chain need to be able to rely on an appropriate business environment. This means, for example, that the principle of technical neutrality of applications must be guaranteed, so that the user is free to choose which application he wants to run on his device, without being limited to the offers made by the provider of the device. Furthermore, the handling of subscribers' data must be clarified. It is unacceptable that e.g. the producer of a Smartphone alone disposes of subscriber information without giving publishers access to the contact details of his client.

III. EPP Group's Demands for the Internet of Tomorrow

The EPP Group puts forward the following **three key demands** for a future EU Internet policy:

1. Coherently apply the principle of transparency.

The EPP Group demands the principle of transparency to be applied by all online actors including ISPs, businesses, data controllers and search engines. For disclosure information to be user-transparent it has to be easily accessible, stated in a clear and simple way as well as verifiable.

2. Strengthen users' online rights.

User rights must be strengthened by informing them about what data are collected for what purpose and for how long they are stored. Awareness raising campaigns must be up-scaled in order to raise users' awareness of possible threats of data abuse.

3. Guarantee fair competition in the Internet.

The EPP Group believes that all commercial Internet actors whether they are located in an EU member state or in a third country need to adhere to EU competition laws. We call upon the Commission to draft legislative proposals addressing the issues of, for example, dominant search engines and traffic management.

The EPP Group's **10 commandments** of the Internet:

1. *Clarify International jurisdiction.* It must be clarified that when ISP collect data within the EU, they have to comply with EU legislation on data protection as well as EU competition law and IPR protection, regardless where these data are stored and/or processed.
2. *Guarantee search neutrality.* Search neutrality must be guaranteed by truthfully disclosing the mechanism underlying the search stated in an easily accessible and understandable way to users. The Commission must investigate the potential abuse of search engine's dominant market position.
3. *Ensure net neutrality.* The neutral transmission of data must be guaranteed regardless of content, origin, application or service which created it. However, it is acceptable for users to choose between different data speeds and volumes. The ban on misleading advertising must be coherently enforced.
4. *Clarify and harmonise data protection rules.* EU data protection rules must be clarified and harmonised at a very high level of data protection. Irrespective of the geographical location of the data controller the principles of transparency, data minimisation, purpose limitation, provision of consent, privacy by design/default and accountability must be applied in the online world. It must be made transparent where data are stored and there must be a deadline for data storage and data use. Awareness-raising and education activities must be developed to ensure that users are properly informed about their rights and obligations.
5. *Ensure users' rights in social networks.* The information which social networks provide to users about purposes and different ways in which personal data is processed must be easily accessible, visible and understandable for the user. Social networks must preset the highest security levels for personal data for each new user registration in line with privacy by default. The right to be forgotten must be properly defined, clarified and guaranteed in the online world.
6. *Prohibit data profiling.* The revised legal data protection framework must forbid data profiling and establish rules for the use of cookies.
7. *Guarantee user anonymity.* ISPs disposing of information allowing for individualisation based on IP addresses must be subject to the same rules and standards applying to telecommunication providers. The collection of location-related data without request must be forbidden.
8. *Design a European Cloud.* The EU should endeavour to legislate on a European Cloud by clarifying issues with regard to standardisation, jurisdiction, security, data protection and privacy. With regard to cybersecurity, the issue of strategic location of data storage needs to be addressed.
9. *Effectively protect IPR online.* The creation of a European framework for IPR has to entail clear rules on copyright licensing, trademark protection and distribution of revenues for all actors including right holders, collecting societies, service providers and consumers; liability schemes need to be reviewed in order to properly protect IPRs.
10. *Establish safeguards for quality journalism.* The Commission is called upon to examine the introduction of ancillary copyright provisions. The technical neutrality of applications must be guaranteed and rules for the handling of subscribers' contact information must be established.