

Ethical aspects of information and communication technologies

Proceedings of the round-table debate

BRUSSELS, 15 NOVEMBER 2011

Ethical aspects of information and communication technologies

NJ-31-11-428-EN-C



HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- via EU Bookshop (<http://bookshop.europa.eu>);
- at the European Union's representations or delegations. You can obtain their contact details on the Internet (<http://ec.europa.eu>) or by sending a fax to +352 2929-42758.

Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

Priced subscriptions (e.g. annual series of the *Official Journal of the European Union* and reports of cases before the Court of Justice of the European Union):

- via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).



European Group on
Ethics in Science and
New Technologies
to the European Commission

Ethical aspects of information and communication technologies

Proceedings of the round-table debate

BRUSSELS, 15 NOVEMBER 2011

Maurizio SALVI
Chief Editor

Head of the EGE Secretariat



EUROPEAN COMMISSION

Maurizo SALVI

Chief Editor

Head of the EGE Secretariat

***Europe Direct is a service to help you find answers
to your questions about the European Union***

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers
or these calls may be billed.

More information on the European Union is available on the Internet (<http://europa.eu>).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2012

ISBN 978-92-79-22327-3

doi:10.2796/13497

© European Union, 2012

Reproduction is authorised provided the source is acknowledged.

Photo © Julien Eichinger

Printed in Luxembourg

PRINTED ON WHITE CHLORINE-FREE PAPER

Contents



INTRODUCTION	
The European Group on Ethics	5
ROUND-TABLE REPORT	7
PROGRAMME FOR 15 NOVEMBER 2011	19
PRESENTATIONS	21
Welcome address by Professor Julian Kinderlerer, EGE President	23
Fabrizio SESTINI <i>Future Internet</i>	25
Chengetai MASANGO <i>The UN Internet Governance Forum</i>	33
Dixie HAWTIN <i>Internet and society</i>	41
William ECHIKSON <i>Internet governance, Google perspective</i>	47
Peter HUSTINX <i>Data protection in an Internet-driven society</i>	63
Lee HIBBARD <i>Council of Europe work on Internet governance</i>	121
Michele BELLAVITE <i>Digital society: an industrial perspective</i>	135
Bernd CARSTEN-STAHl <i>Ethics and future Internet</i>	139
Guido VAN STEENDAM <i>Social determinants of ICT</i>	145
ANNEX I	
Participants	167
ANNEX II	
Secretariat of the European Group on Ethics	171



Introduction

The European Group on Ethics

The European Group on Ethics in Science and New Technologies (EGE) is an independent, pluralist and multidisciplinary body which advises the European Commission on ethical aspects of science and new technologies in connection with the preparation and implementation of European Union legislation or policies.

The group is made up of 15 independent experts appointed by the Commission for their expertise and personal qualities.

The EGE was set up by the European Commission in December 1997, to succeed the Group of Advisers on the Ethical Implications of Biotechnologies (GAEIB, 1991–97). During its first term (1998–2000), the EGE gave opinions on subjects as diverse as human tissue banking, human embryo research, personal health data in the information society, doping in sport and human stem cell research.

In April 2001, the Commission appointed 12 members for the period 2001–04. During its second term, the group published opinions on the ethical aspects of patenting inventions involving human stem cells (Opinion No 16 — 7 May 2002), clinical research in developing countries (No 17 — 4 February 2003), genetic testing in the workplace (No 18 — 28 July 2003) and umbilical cord blood banking (No 19 — 16 March 2004).

On 11 May 2005, the Commission decided to renew the Group's mandate for a further four-year period. For this third term, the EGE was increased in size from 12 to 15 members. In the same year the group published its

opinion on the ethical aspects of ICT implants in the human body (No 20 — 16 March 2005). So far in this term the EGE has given opinions on ethics and nanomedicine ⁽¹⁾ (No 21 — 17 January 2007), an ethics review of seventh framework programme (FP7) human embryonic stem cells projects ⁽²⁾ (No 22 — 13 July 2007), the ethical aspects of animal cloning for food supply (No 23 — 16 January 2008), the ethics of modern developments in agricultural technologies ⁽³⁾ (No 24 — 17 December 2008) and the ethics of synthetic biology ⁽⁴⁾ (No 25 — 17 November 2009), as well as its general activity report ⁽⁵⁾ (September 2010).

On 10 January 2011, the President of the European Commission José Manuel Barroso appointed the 15 members of the EGE ⁽⁶⁾ for 2011–16. The selected members serve in a personal capacity and are asked to offer independent advice to the Commission ⁽⁷⁾. On 22 March, Mr Barroso requested the EGE to issue an opinion on the ethical implications of information and communication technologies (ICT). He also asked for an opinion on the ethical implications of security and surveillance technologies.

When preparing its opinions, the EGE engages in a broad consultation, involving individual experts, representatives of European institutions, of other international institutions and of civil society and the chairs of the national ethics councils in the European Union Member States. The group organised a round table in Brussels on 15 November 2011 in order to promote a transparent dialogue between parties representing many different interests. This report gives a summary of the presentations and discussions.

⁽¹⁾ http://ec.europa.eu/bepa/european-group-ethics/docs/publications/opinion_21_nano_en.pdf.

⁽²⁾ http://ec.europa.eu/bepa/european-group-ethics/docs/publications/opinion_22_final_follow_up_en.pdf.

⁽³⁾ http://ec.europa.eu/bepa/european-group-ethics/docs/opinion24_en.pdf.

⁽⁵⁾ http://ec.europa.eu/bepa/european-group-ethics/docs/gar_ege_2005-2010_web.pdf.

⁽⁶⁾ The EGE consists of 15 members. They are appointed on the basis of their expertise and a geographical distribution that reflects the diversity in Europe. EGE Members are nominated *ad personam*; they do not represent Member States, political parties, lobby groups or religions.

⁽⁷⁾ http://ec.europa.eu/bepa/european-group-ethics/welcome/mandate-2011-2016/index_en.htm.



Round-Table Report

1. Main goal of the round table

The European Group on Ethics in Science and New Technologies (EGE) is preparing an opinion on the **ethical aspects of information and communication technologies**. As part of its preparatory work, the EGE held an open round-table debate on the issues raised by ICT. The round table was organised by the Bureau of European Policy Advisers (BEPA).

As was the case for previous EGE opinions and in accordance with the Commission decision on the EGE's mandate (Decision 2005/383/EC), a public round table was organised to debate openly the ethical, social and legal implications of ICT. The main goal was to give stakeholders an opportunity to provide the EGE with relevant data, considerations and viewpoints before finalisation of Opinion 26, which is to be adopted in February 2012.

2. The round table

The European Group on Ethics in Science and New Technologies (EGE)

The EGE was established in 1991 (with the name of the Group of Advisers on the Ethical Implications of Biotechnology (GAEIB), and the new EGE mandate was adopted by a Commission decision on 23 December 2009⁽⁸⁾ (2010/1/EU). According to the above remit, the role of the EGE is to provide the Commission with high-quality and independent advice on the ethical aspects of science and new technologies in connection with the preparation and implementation of European Union legislation or policies⁽⁹⁾.

On 10 January 2011, the President of the European Commission José Manuel Barroso appointed the 15 members of the European Group on Ethics in Science and New Technologies (EGE) for 2011–16. The selected EGE members serve in a personal capacity and are asked to offer independent advice to the Commission⁽¹⁰⁾. They have been appointed on the basis of their expertise and a geographical distribution that reflects the diversity in Europe. The EGE held its first meeting on 8 and 9 February in Brussels and had a session with President Barroso. A second meeting took place on 15 and 16 March, also in Brussels. Professor Julian Kinderlerer was elected as the group's President and Professor Linda Nielsen as Vice-President. Rules of procedure were adopted on 15 March.

The EGE opinion on the ethics of ICT

At the request of the President of the European Commission, the EGE is currently working on an opinion on the ethics of information and communication technologies⁽¹¹⁾, which will provide the Commission with policy options for the governance of ICT.

The EGE held its third meeting on 12 and 13 April, its fourth meeting on 17 and 18 May and its fifth meeting on 21 and 22 June, all in Brussels⁽¹²⁾. The forthcoming opinion on ethics and ICT was discussed with the chairs of the EU-27 national ethics councils on 21 September. The EGE was then due to have a number of working meetings in November and December 2011 and January 2012, before the final approval of the opinion in February 2012.

⁽⁸⁾ The EGE's mandate was renewed by the Commission decision of 26 March 2001 for a four-year period and its remit was slightly modified to improve the group's working methods. The EGE's mandate was decided on 11 May 2005 (Decision 2005/383/EC), and extended by a Commission decision of 14 October 2009 (Decision 2009/757/EC). Members of the European Parliament cannot be selected as EGE members because this may determine conflict of interest and would contradict provisions stated in the remit of the group (Legal Service (JUR(2006)30358 JFP/fag, dated 3.7.2006).

⁽⁹⁾ The Parliament and the Council may draw the Commission's attention to questions which they consider to be of major ethical importance.

⁽¹⁰⁾ http://ec.europa.eu/bepa/european-group-ethics/welcome/mandate-2011-2016/index_en.htm

⁽¹¹⁾ The President of the European Commission has also asked the EGE to issue an opinion on the ethical implications of security and surveillance technologies. Following the last Competitiveness Council on the Euratom programme, the Commission is considering asking the EGE to contribute to the debate on a sustainable energy mix in Europe by issuing an opinion on the ethical impact of research on different energy sources on human wellbeing.

⁽¹²⁾ http://ec.europa.eu/bepa/european-group-ethics/welcome/activities/index_en.htm.



The EGE round table on ethics in ICT

When preparing its opinions, the EGE engages in broad consultation, involving individual experts, representatives of European institutions, other international institutions and civil society and the chairs of the national ethics councils in the European Union Member States.

It organised a round table on 15 November 2011, at the European Commission, in the Robert Schuman Room at the Berlaymont Building at Rond Point Schuman in Brussels.

Participants came from a broad cross-section of European society, including the scientific community, industry, civil society, policymakers, media and the general public. Invited speakers included: **Fabrizio Sestini** (European Commission, Directorate-General for the Information Society and Media); **Chengetai Masango** (UN Internet Governance Forum); **Dixie Hawtin** (Research and Policy, Global Partners and Associates); **William Echikson** (External Relations, Communications and Public Affairs, Head of Free Expression EMEA at Google); **Peter Hustinx** (EU, European Data Protection Supervisor); **Lee Hibbard** (Council of Europe's coordinator on the information society and Internet governance); **Michele Bellavite** (European Telecommunications Network Operators' Association (ETNO), Chairman of the Digital Society Working Group); **Bernd Carsten Stahl** (Director of the Centre for Computing and Social Responsibility, De Montfort University); **Guido Van Steendam** (Professor of the Philosophy of Technology, KU Leuven, and Director, International Forum for Biophilosophy (IFB)).

Report of the EGE round table

Professor Julian Kinderlerer, the EGE President, chaired the meeting. He welcomed participants and explained the group's new remit for 2011–16. He said this has

been extended to the ethics of science and technology as a whole and not only biomedicine or biotechnology, as in the past. He explained that on 21 March 2011 President José Manuel Barroso had asked the EGE to draft an opinion on the ethical issues arising from the rapid expansion of information and communication technologies (ICT). President Barroso indicated that the opinion could 'offer a reference point to the Commission to promote a responsible use of the digital agenda for Europe and facilitate the societal acceptance of such an important policy item'. The EGE accepted the request and decided to mainly focus on Internet technologies.

Professor Kinderlerer then underlined that the EGE promotes open and transparent dialogue with relevant stakeholders. He said that, in addition to what it had received in the hearings it had organised and the meeting with the chairs of the EU-27 national ethics councils, the group was aiming to get critical arguments and inputs for the requested opinion.

Dr Sestini (Information Society and Media DG) made a presentation on future uses of the Internet. He said that understanding the Internet, as the biggest artefact of humankind, requires competences coming from both the life and human sciences, that are not limited to technological or infrastructural aspects, but also include sociology, art, policy and economy. This is due to the fact that Internet is bringing about radical changes such as economic transformation, social expansion, psychological changes and new legal aspects. All these competences are required to understand how the Internet is going to look in the future, and in particular to determine if and how it may help the transition towards a more sustainable future (in environmental, economic or social terms), which can in itself be seen as an ethical aspect. Dr Sestini presented two extreme scenarios developed in a recent study on the future Internet carried out by the University of Oxford: the 'Big Brother', where

the Internet is evolving towards a purely commercial, centrally controlled entertainment-delivery infrastructure, and 'collective awareness' (see also the upcoming related initiative at http://ec.europa.eu/information_society/activities/collectiveawareness), where it is evolving towards an open and distributed discussion platform to share information and collectively produce content and awareness, contributing to social and democratic life. The emergence of such scenarios can be linked to key technological and policy choices, such as network architectures, security policies, digital intellectual property rights (IPR) approaches, open standards and network neutrality. He concluded with a quick overview of all the technological, application or policy choices which may involve significant ethical aspects, as they can drive future Internet developments more towards the fulfilling of societal needs rather than commercial objectives. The list included elements such as: community networks; cloud strategy; autonomic networks; next generation networks (NGN); safeguarding the end-to-end principle; quality of service (QoS); deep packet inspection (DPI); freedom of expression; privacy, trust and reputation; identity management; security; environmental monitoring; customer control and profiling; sensor networks; the Internet of Things (IoT); ambient intelligence; peer to peer (P2P); IPR; and open standards.

Following Dr Sestini's presentation, there was a debate on topics including:

- the impact of the Internet on human culture;
- actions to promote education about the Internet;
- the use of the Internet for policymaking purposes.

Dr Masango (United Nations) reported on the United Nations Internet Governance Forum (IGF). He explained that the UN started to work on Internet governance in 2003 and established the IGF as a multi-stakeholder debate forum with no normative powers. In 2010, the remit of the IGF was extended until 2015. The forum aims to create an interdisciplinary platform where NGOs, industry and governments debate issues at paritetic level. The next meeting will be in Baku in 2012. Dr Masango explained that Internet governance implies actions by government, civil society and private enterprises. He also underlined that shared principles, norms and rules are key elements to promote a proper governance of the Internet and recalled that Unesco has addressed the ethical considerations of ICT. He then underlined that dynamic coalitions across relevant stakeholder groups so far established via the IGF include: open standards; Internet rights; freedom of expression; and media and child online safety.



Following Dr Masango's presentation, there was a debate on topics including:

- the possibility to establish minimal normative standards at UN level (Internet governance);
- awareness-raising processes;
- the role the Universal Declaration of Human Rights plays in the debate over Internet governance;
- the current debate on the role the UN may play in Internet governance (institutional level).

Dixie Hawtin (Global Partners and Associates) made a presentation on the Internet and society. She explained that democratic freedom of expression and the Internet aim to receive free information. She underlined that the Internet was created in a libertarian spirit, but governments have now realised its potential and its control is being promoted by several actors (governments and multinationals) for commercial interests. She advocated that three values should be promoted in Internet governance: (1) global public value; (2) a multi-stakeholder approach; and (3) a space of human rights protection. She explained that governments around the world are now alert to the potential disruption caused by access to digital communications. Many less democratic governments are seeking to control and monitor the online space with new tools such as: filtering and blocking; registration requirements; surveillance powers; intermediary liability; and persecuting users in real life. She stated that China and Russia are preparing Internet security protocols and that Internet governance is now being debated in organisations dominated by developed countries (OECD), jeopardising both the role UN is having in this global governance effort and the role developing countries may play in international debates. She underlined that the European Union should make a strong investment in the multi-stakeholder approach in

contrast to actions being established by OECD and the Council of Europe in order to adopt normative documents with no participation by non-governmental organisations and other non-institutional stakeholders from different regions of the world. She also underlined that IPR is a key issue to address, in particular with regard to developing countries where high risks of e-exclusion exist.

She concluded by stating that access to information is a key element to preserve and that we should be driven by an understanding of the Internet as a global public value space; multi-stakeholder actors should be protected in order to achieve a proper Internet governance and human rights should apply to the Internet domain. She indicated some useful approaches in Internet governance, namely: (1) to promote discussion and build consensus; (2) to allow countries/institutions to coordinate policy efforts which protect flexibility and innovation; and (3) to tend to be less formal than, say treaties, allowing more involvement of civil society.

Dr Echikson (Google) made a presentation on Google's views on Internet governance. He noted that 2 billion people can express themselves daily via the Internet, there are 325 billion websites and 70 000 pictures are downloaded every minute. He underlined that the Internet is the most powerful communication tool in history. Blogs, social networks and online video platforms are now widely available for everyone with access to it.

Dr Echikson said that repressive governments are determined to block this free flow of information. At Google, they saw technology used to stifle speech every day. He explained that Google products, from search and Blogger to YouTube and Google Docs, have been blocked in more than 25 of the approximately 150 countries where they offer their services. At least 17 countries have blocked YouTube at some time and it is still fully blocked in China, Iran and North Korea. He also reported that Google

employees have been convicted in Milan in a criminal case that represents a severe threat to the freedom of the Internet and is inconsistent with both Italian and European Union law. The conviction stems from an incident in 2006 when students at a school in Turin filmed and then uploaded a video to Google Video that showed them bullying a disabled schoolmate. He explained that in Iran the government closed down the Internet system during political rebellions. He stated that in navigating online speech, two guiding principles should be kept in mind. The primary responsibility is to Internet users, to maximise their access to information and provide an open platform for their free expression. The second is the principle of transparency. He mentioned the Google Transparency Report (<http://www.google.com/transparencyreport/>) established in 2010 and featuring data, listed on a country-by-country basis, of the number of requests received from governments to either hand over data about Google users or remove content.

Dr Echikson explained that in 2009 Google joined negotiations with Microsoft, Yahoo, human rights groups and others in the USA to try to arrive at a code of conduct for how technology companies operating in countries with repressive regimes could best operate to promote freedom of expression and protect the privacy of users. The result, called the Global Network Initiative, holds companies accountable for their commitments to protect their users and maximises the power of its membership to effect change and prevent backsliding. Yet so far, no European company has signed up. He concluded by stating that Google's aim for preserving the openness of the Internet is to get governments to embrace its power and not try to stop it in recognition that the Internet can be a powerful tool to advance their economies and improve the lives of their citizens.

He advocated the need for European political support for freedom of expression as well as launching a proper debate on Internet governance in the EU.

Following the presentation, there was a general debate on topics including:

- normative intervention to control information in emergency cases;

- the notion of freedom of expression in ICT;
- the potential clash between privacy and copyright on the Internet (including the debate on open source);
- the right to be connected;
- freedom of expression and child pornography on video;
- the right to be forgotten;
- privacy by design (the link between transparency and consumer interests);
- the rule of law in the EU and guidelines prepared by governmental bodies;
- the involvement of users in ICT design;
- the embedding of ethics in Internet technology design;
- the control of open Internet platforms;
- consent forms and individual rights;
- the role of information providers and risks of monopolies;
- human rights versus cybersecurity;
- access to new ICT products in Africa and the less developed regions of the world.
- the tension between human rights and law enforcement provisions in ICT;
- different interpretations of freedom of expression in different regions of the world;
- the concept of multi-stakeholder governance and actions to bypass it when powerful stakeholders (governments, corporations) feel in danger;
- the empowerment of law on the Internet;

- data protection and cloud computing;
- the neutrality of the Internet;
- Internet providers' responsibility and mechanisms to implement it;
- open access issues and their role in developing countries.

Dr Hustinx (European Data Protection Supervisor, EDPS) made a presentation on data protection in an Internet-driven society. He mentioned the importance of the opinion on Internet neutrality issued by the EDPS in October 2011. He explained that 27 data protection authorities deal with the national compliance of EU data protection regulatory frameworks and that the EDPS addresses the EU dimension of this issue. He stated that a review of the data protection directive is ongoing, and is a top priority of the EU Vice-President and Commissioner for Justice, Fundamental Rights and Citizenship Viviane Reding. He underlined that the Lisbon Treaty⁽¹³⁾ (Article 16) has introduced a stronger role for data protection in the European Union but globalisation is complicating the notion of territoriality and law enforcement (think of ICT and cloud computing).

He stated that responsibility is the main issue to address, both as a value and as an element having legal significance. The enforcement of data protection law, he said,

needs incentives for compliance and measures for infringements (accountability issues). He stressed the need for reinforcing tools for implementing existing legal data protection measures. The rights of data subjects have to be reinforced and their exercise in practice facilitated, while transparency is needed by the controllers (including informed and reversible consent procedures). Dr Hustinx explained that national data protection supervisory authorities in the EU have different levels of autonomy and powers, but advocated uniform standards for independence and enforcement powers to ensure a harmonised transparent approach to data protection⁽¹⁴⁾. He stated that a regulation or a directive for law enforcement may be proposed in January by the Commission and that effectiveness, transparency and harmonisation are all elements in the new regulatory frameworks.

He then approached issues related to Internet neutrality (the idea that Internet providers should not interfere with the content and the place of the information conveyed on Internet) and stressed that 'traffic management' tools often violate EU data protection provisions. There is a need for greater clarity on the distinction between legitimate (for example, protection from viruses) and unacceptable screening techniques, including 'deep packet inspection'. He concluded that screening of messages is often a tool to monitor the content of communications and that telecom providers have to comply with data protection rules.

⁽¹³⁾ Treaty on the Functioning of the European Union.

⁽¹⁴⁾ He stated that UK has 300–400 breaches of rules every year. Some 80 % of cases refer to lack of ownership of data and technical features. Sanctions are needed as well as measures to prize proper respect of data protection measures.



Following Dr Hustinx's presentation, there was a debate on topics including:

- legal enforcement provisions for data protection;
- territoriality and protection of data protection in cloud computing and among EU consumers outside the EU;
- data protection provisions in the EU, USA, Africa and China;
- confidentiality of personal data on the Internet (privacy);
- responsibility and accountability on the Internet.

Dr Hibbard (Council of Europe, CoE) made a presentation on Internet governance activities at the Council of Europe. He underlined that privacy on the Internet is a key to address (cloud computing) and that this impacts on the notion of democracy. He stressed the need for mutual reinforcement between European Commission and CoE actions on human rights protection (including the Internet).

He underlined that human rights also have to be respected in the digital world and that several international bodies are addressing this issue, including the OECD, World Bank and NATO.

He stressed that Article 10 of the European Convention on Human Rights affirms the right of freedom of expression and responsibility for its infringement. He recalled the magnitude of the problem, with 2 billion Internet users and 700 million of Facebook. He referred to a number of legal cases such as those in France (Hado-pi), Italy (Google) and Turkey (YouTube), where Internet providers have been prosecuted for the content of

information introduced on the Internet. He pointed out that Unesco has prepared a code of ethics on the information society and stressed the need for shaping ethical understanding of the ICT in the EU and globally.

He stressed that an ethical process requires bottom-up multi-stakeholder dialogue policy processes. He announced that the Council of Europe will work on search engine provider guidelines, social network provider guidelines and a user's charter and on the ethics of the ICT private sector. He recalled that the Council of Europe ethical principles on Internet declaration were adopted in September 2011.

Dr Bellavite (ETNO) reported on the industrial perspective of the Internet governance debate. He explained that ETNO clusters 42 telecom companies in the EU and said that while the topics on Internet governance are not new, the relevance this debate is acquiring is a new phenomenon (previous topics include liberalisation of the markets, price setting and access regulations).

He said that, as regards governance of the Internet, ETNO fully supports a multi-stakeholder approach with no regulatory oversight by any Government entity, considering that the challenges of Internet governance and principles mainly concern its global reach and nature. This collaborative, bottom-up approach is fitting in view of the global nature of the Internet. The recent emergence and development of high-level Internet principles (e.g. the OECD Principles on Internet Economy, the Aspen Principles for the Future of the Internet) is helpful in setting out best practice and guidelines for the online world. It is therefore important that the EU starts a reflection on how it can make sure that European values and human rights traditions can be safeguarded on a global level.

Dr Bellavite stressed that the public policy debate on the Internet is increasingly centred on the relationship

between the end-user and the online world/service providers and indeed on appropriate behaviour online. Many argue for applying in the online world the same level of protection afforded in the offline world. Telecom players are already committed to provide transparent and meaningful information regarding their offers and, in particular, any limitations on consumers' ability to access content and/or applications of their choice, further strengthening consumer choice in this field. In addition, the telecoms regulatory framework offers numerous consumer protection safeguards, such as the contractual rights set out in the citizens' rights directive. He explained that ETNO believes that no further regulatory intervention is needed and that it is important to allow

industry the freedom to innovate and adopt new business models and services in a fast-moving technology environment.

He stressed that the digital agenda targets provision of high-speed Internet in the EU as a key priority for industry, but said this requires a conducive regulatory framework to foster investment.

He also stressed that the role of regulators for new technologies should reflect the plastic evolution of the technological tools under consideration, remaining technologically neutral.



Following the presentation, there was a general debate on topics including:

- Internet neutrality and different kinds of Internet users;
- technology neutrality;
- corporate responsibility and soft law governance models;
- minimal regulatory requirements welcomed by the ICT industry.

Professor Carsten-Stahl (Professor of Critical Research in Technology and Director of the Centre for Computing and Social Responsibility, De Montfort University) spoke about the ethics of new Internet technologies. He reported on an EU-funded project (ETICA) that addresses new ICT domains from an interdisciplinary point of view and explained that new features of emerging ICT include natural interaction, invisibility and a detailed understanding of users, pervasive and autonomous. Some of the predictable ethical issues of emerging ICTs include privacy, security, trust, liabilities and digital divides, and he said that many of these will take new forms. Privacy, for example, is likely to become even more prominent due to new quantities of data, new ways of linking it and maybe even new types of data (e.g. emotional data) which may raise qualitatively new issues. What these issues have in common, however, is that they are currently on the social and political agenda and are recognised as important and in need of further attention.

Professor Carsten-Stahl also addressed what he called less predictable ethical issues arising from the emerging ICTs and said that they tend to be centred on difficult conceptual issues, such as human identity, the relationship between humans and technologies, and relationships among individuals or groups. Individual

identities may change due to the way we interact with technology. What we perceive to be normal is partly a function of the affordance that technologies offer us and therefore potentially subject to change. A good example for this is the difficult distinction between therapy and human enhancement. Related issues can arise due to the way in which new technologies can change power relationships and traditional balances between individuals and groups. In extreme cases, such changes can affect not only local cultures and collective self-views but also the ways in which societies organise and reproduce themselves. This does not have to be morally problematic, but it may well be in some respects. The scale of the change means that potential ethical issues need to be monitored closely.

He also stressed that the majority of ICT moral issues are technology and context-dependent. He explained that diverging perceptions of technologies and their affordances as well as different sociomaterial enactments of sociotechnical networks preclude an abstract and decontextualised appreciation of what the real issues will turn out to be. He said that governance arrangements that are used to identify and address ethical issues of emerging ICTs must be flexible and open to development and deliberation. They need to be able to combine ethically justified procedures with guidance on local and established moral issues and examples of their resolution.

He explained that some of the issues to consider include security, trust, liability and digital divide, enhancement, normality, mortality, identity, power relationships, the environment, the nature of society and changing cultures. He advocated that ethical impact assessment should be requested in normative frames to apply to ICT. He also underlined that the EGE opinion should consider that ICT is more than Internet governance and additional ethics debates will be needed in other applications of ICT.

Professor Van Steendam (Professor of the Philosophy of Technology, KU Leuven and Director, International Forum for Biophilosophy) made a presentation on the social determinants of information and communication technologies. He focused on the difference between (a) using information as abstract material and (b) dealing with information as part of embodied and embedded human activities. Much of the strength and efficiency of the Internet and ICT lies in their objective of using abstract information (building on Claude Shannon's mathematical theory of information and communication). He remarked, however, that this ideal of abstract information is also a major reason why ICT gets dissociated from real life concerns and becomes a major source of ethical issues. To properly address ethical issues linked to ICT, he underlined, we have to consider information as an embodied and embedded reality. He first illustrated this point in the context of compiling and organising information. In this process we often perceive information as 'material units' that can be collected and combined to build up intelligence. While our society has learned that this compilation of information has its own value, we are also aware of its limits. We realise that information is more than the mere material that can be stored on a hard disk. In real life, the same material information can trigger different actions and understandings, depending on the specific way in which people who receive the information are embodied and embedded. The meaning of the information depends on the physical conditions of the people who are informed, on their ambitions and plans, available infrastructure and contacts and many other elements that identify their activity world. The intelligence people develop in their lifetime is only intelligent in their own body and social and natural context. Should we be able to transfer the intelligence of an experienced and wise older Indian woman to a young American boy, this boy would not become intelligent. He has to build up his own intelligence. Ignoring this weakens the

real-life social impact of ICT and raises ethical issues. When Google more or less succeeds in identifying some dozens or hundreds of relevant documents selected from the millions of possible documents available in cyberspace, the reason is not that Google has superior tools to analyse the abstract information online, but that it uses the intelligence of its embodied and embedded users by analysing their clicking behaviour, preferences and assessments.

As a second illustration, Professor Van Steendam discussed the process of communication of information. In an abstract vision of information, transfer of information is compared to the flow of dead material from one context to another. When we realise that information is always embedded, the transfer means that information is detached from its original meaning in one embedded context and is injected into a new embedded context. In this new context, the transferred information acquires a new meaning. Quite often people feel that information 'is taken out of its context'. We now realise that such a change of meaning is not only happening on exceptional occasions. Information that is re-told or transferred is **always** taken out of its context. This unavoidable aspect of communication requires special attention, and there are no easy solutions for finding out which changes of meaning are acceptable or unacceptable.

The last illustration presented is the role of people in the process of information transfer. In an abstract view of information, the flow of information is seen as the active agent, while the people are seen as the passive medium through which information is flowing. In real life, people never passively absorb information. They are the active and enthusiast agents who actively absorb, reinterpret and transfer information. When an ethical analysis does not address this active process, we miss the most important ethical issues linked to information and communication technologies.



Following the presentation, there was a general debate on topics including:

- the decontestalisation of information;
- critical infrastructure protection of digital information;
- the notion of dependency in the Internet domain;
- the notion of a homogenous society and its link with complexity;
- identity and identification in the Internet;
- embedding information and people in the Internet;
- the implementation of the digital agenda and the role ethics may play in this process.

Professor Kinderlerer delivered the final conclusions. He thanked participants and stressed that that the EGE will take into due considerations all the inputs it has received.

A video of the round table is available on the EGE website ⁽¹⁵⁾.

Maurizio SALVI, PhD,
Head of the EGE Secretariat

⁽¹⁵⁾ http://ec.europa.eu/european_group_ethics/activities/index_en.htm.

Programme

Brussels, 15 November 2011

- 09.30 **Registration**
- 10.00–10.10 Welcome address by **Julian Kinderlerer**
President of the EGE
- 10.10–10.30 **Future Internet**
Fabrizio Sestini (European Commission,
Directorate-General for the Information
Society and Media)
Followed by discussion (10 minutes)
- 10.30–10.50 **The UN Internet Governance Forum**
Chengetai Masango (Programme
and Technology Manager, UN Internet
Governance Forum)
Followed by discussion (10 minutes)
- 10.50–11.10 **Internet and society**
Dixie Hawtin (Research and Policy, Global
Partners and Associates)
Followed by discussion (10 minutes)
- 11.10–11.30 **Internet governance, Google perspective**
William Echikson (External Relations,
Communications and Public Affairs, Head
of Free Expression EMEA at Google)
Followed by discussion (10 minutes)
- 11.30–12.00 **Coffee break**
- 12.00–13.00 Discussion and contributions from
participants
- 13.00 **Lunch**

Afternoon session

- 14.30–14.50 **Data protection in an Internet-driven
society**
Peter Hustinx, (EU, European Data
Protection Supervisor)
Followed by discussion (10 minutes)
- 14.50–15.10 **Council of Europe work on Internet
governance**
Lee Hibbard (Council of Europe's
coordinator on the information society
and Internet governance)
Followed by discussion (10 minutes)
- 15.10–15.30 **Digital Society: an industrial perspective**
Michele Bellavite (European
Telecommunications Network Operators'
Association (ETNO), Chairman of the
Digital Society Working Group)
Followed by discussion (10 minutes)
- 15.30–16.00 **Coffee break**
- 16.00–16.10 **Ethics and future Internet**
Bernd Carsten-Stahl (Professor of Critical
Research in Technology and Director
of the Centre for Computing and Social
Responsibility, De Montfort University)
- 16.10–16.20 **Social determinants of ICT**
Guido Van Steendam (Professor of the
Philosophy of Technology, KU Leuven;
Director, International Forum for
Biophilosophy)
- 16.20–17.20 Discussion and contributions from
participants
- 17.20–17.30 Closing remarks from the EGE President
- 17.30 **End of the round table**

The round table was broadcast on <http://webcast.ec.europa.eu>

Presentations



**Ethical aspects of information
and communication technologies**



Ethical aspects of information and communication technologies



Julian KINDERLERER

President, European Group on Ethics
in Science and New Technologies

Julian Kinderlerer is:

1. Professor of Intellectual Property Law and head of the research unit on IP law in the Department of Private Law, University of Cape Town;
2. Professor of Biotechnology and Society in the Technology University in Delft, the Netherlands;
3. former Professor of Biotechnology Law and former Director of the Sheffield Institute of Biotechnological Law and Ethics in the University of Sheffield;
4. President of the European Group on Ethics in Science and New Technologies (EGE) that advises the European Parliament, the Council and the Commission on ethical issues in relation to new science and technologies (http://ec.europa.eu/european_group_ethics/index_en.htm).

He is a biochemist who moved from research interests in the theoretical aspects of enzymology and enzyme kinetics to looking at law, ethics, risk assessment and risk analysis in biotechnology, and then to leading a group at UCT on intellectual property law and policy.

He is the President of the European Group on Ethics in Science and New Technologies (EGE) that reports to the European Parliament and to the President and Council of the European Union. In February 2009, he was the legal adviser to the small team representing South Africa that was involved in negotiating a new international treaty on liability and redress in the event of harm caused by living modified organisms that have their origin in transboundary movement between countries. At the negotiations he took the lead on behalf of South Africa and was part of the African delegation that was allowed a total of six negotiators at the table. The negotiations eventually led to the Nagoya–Kuala Lumpur Supplementary Protocol on Liability and Redress

to the Cartagena Protocol on Biosafety that was agreed last year by the parties to the Convention on Biological Diversity and the Biosafety Protocol. Julian has advised the South African Department of Science and Technology. Globally he has attended (and chaired) an inter-agency group involving the UN organisations, the World Trade Organisation and the European Union looking at the ethical issues of intellectual property protection and has advised and worked with the European Patent Office (EPO) in relation to biotechnology patents. During June 2009, he was invited to work with the directors of the EPO biotechnology teams at a retreat looking at patents in this important area.

During 2000, he was seconded to work in Nairobi for the United Nations Environment Programme, and prepared a project that has been funded by the Global Environment Facility (GEF) to assist in the provision of biosafety frameworks in 119 developing countries. He was also one of the prime authors of the initial strategy for biosafety agreed by the GEF. He remained involved as the primary 'consultant' for the project and works with and in many of the 124 countries involved in the development phase of the project. He was the specialist adviser, during 1998, to a House of Lords Select Committee investigation into modern biotechnology with particular reference to European law as it impacts on agriculture and food. This was a major report on the manner in which European legislation in relation to genetically modified organisms should be handled.

Julian was a member of the Advisory Committee for Genetic Modification (ACGM) from 1984 to 2003, a member of the independent technical subcommittee of ACGM till 2003 and a member of the Advisory Committee for Releases into the Environment (ACRE) since releases were first considered in the UK until 1999. He has contributed to the drafting of legislation or guidelines for the safe use of the products of biotechnology in many countries, including Malaysia, Thailand, the Baltic states, Russia, Bulgaria, the Czech Republic, Namibia, South Africa, Mexico and Brazil.

Opening by Julian Kinderlerer, President of the European Group on Ethics of Science and New Technologies

Every day, more than 250 million Europeans are connecting to the Internet, to work, learn, communicate, play and socialise. But the digital economy which has rapidly grown up around all those activities poses new challenges to governments and regulators. Business models are likely to change significantly as Internet access permits comparison of goods and prices and the ability to shop across borders. Work and play will also change dramatically as personal interaction changes from word of mouth and personal meetings to include interactions unlimited by place or time. Communication and mechanisms for interacting with others are already changed beyond recognition, and will almost certainly continue to change at an accelerating pace. The digital revolution will impact on everything people do, including life choices, health, shopping, education and communication. Most importantly, national and regional boundaries are being diluted and will continue to be through the speed and accessibility of new technologies.

On 21 March 2011, President José Manuel Barroso asked the EGE to draft an opinion on the ethical issues arising from the rapid expansion of information and

communication technologies (ICT). President Barroso indicated that the opinion could 'offer a reference point to the Commission to promote a responsible use of the digital agenda for Europe and facilitate the societal acceptance of such an important policy item'. The EGE accepted the request and decided to focus mainly on Internet technologies. This opinion should provide suggestions for an ethically sound use of ICT.

Before finalising each EGE opinion, the group discusses the subjects with relevant stakeholders (industry, civil society, patients, NGOs, representatives of churches and religious groups, etc.). To allow this consultation step, today's round table has been organised prior to the adoption of the EGE opinion. The round table is open and structured in such a way that participants have the time and opportunity to speak directly to EGE members on issues they feel deserve specific attention by the group in preparing its opinion. To maximise the participation in the discussion, the round table is being web streamed and a written consultation on ethics and ICT has been launched. I thank you all for coming here today and look forward to your comments and suggestions.



Ethical aspects of information and communication technologies



Fabrizio SESTINI

Scientific Officer, European Commission,
Directorate-General for the
Information Society and Media

Fabrizio Sestini is a scientific officer with the Information Society and Media DG of the European Commission. He has been involved in the definition and management of several research initiatives related to different aspects of future Internet developments, including mobile Internet access, new paradigms for Internet infrastructures (also as part of 'Future and emerging technologies' — FET) and experimental facilities.

His current interests are in the social and ethical implications of future Internet technologies, and in the definition of new multidisciplinary research priorities with high social and economic impact. In particular, he is launching a new area called 'Collective awareness platforms for social innovation and sustainable social changes', and he is in charge of the multidisciplinary 'Network of excellence in Internet science', aiming to better understand the complex interrelation between technological developments and the socioeconomic impacts of the Internet.

In previous years, he has developed and launched SAC ('Situating and autonomous communications'), a FET Proactive initiative launched in 2004, and FIRE ('Future

Internet research and experimentation'), a flagship initiative launched in 2007. In 2009 and 2011, he was the European Commission organiser of the Paradiso 'ICT for a global sustainable future' high-level events, proposing that ICT developments be focused to solve the sustainability issues of society and the planet.

Before joining the Commission, Fabrizio received both his PhD in information and communication engineering and his degree in electronic engineering from the 'La Sapienza' University of Rome. He worked with CSELT (now Telecom Italia Lab) in Turin on the adaptation of dynamic channel allocation techniques to the existing GSM network, and later with RAI, the Italian public broadcasting company, developing data broadcasting systems and services in collaboration with IBM and Olivetti.

Fabrizio is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), holds an industrial patent, has served on the Technical Program Committee (TPC) of several international conferences and is the author of more than 30 scientific papers, mostly published in IEEE journals and in conference proceedings.

Future Internet

Fabrizio SESTINI

Future Internet: ethical aspects



Drawing made by primary class children for the Paradiso contest “the **Internet of the future** seen by the children of today”

Fabrizio.Sestini @ ec.europa.eu

http://cordis.europa.eu/fp7/ict/fire/future-internet-and-society_en.html

European Commission DG Information Society & Media

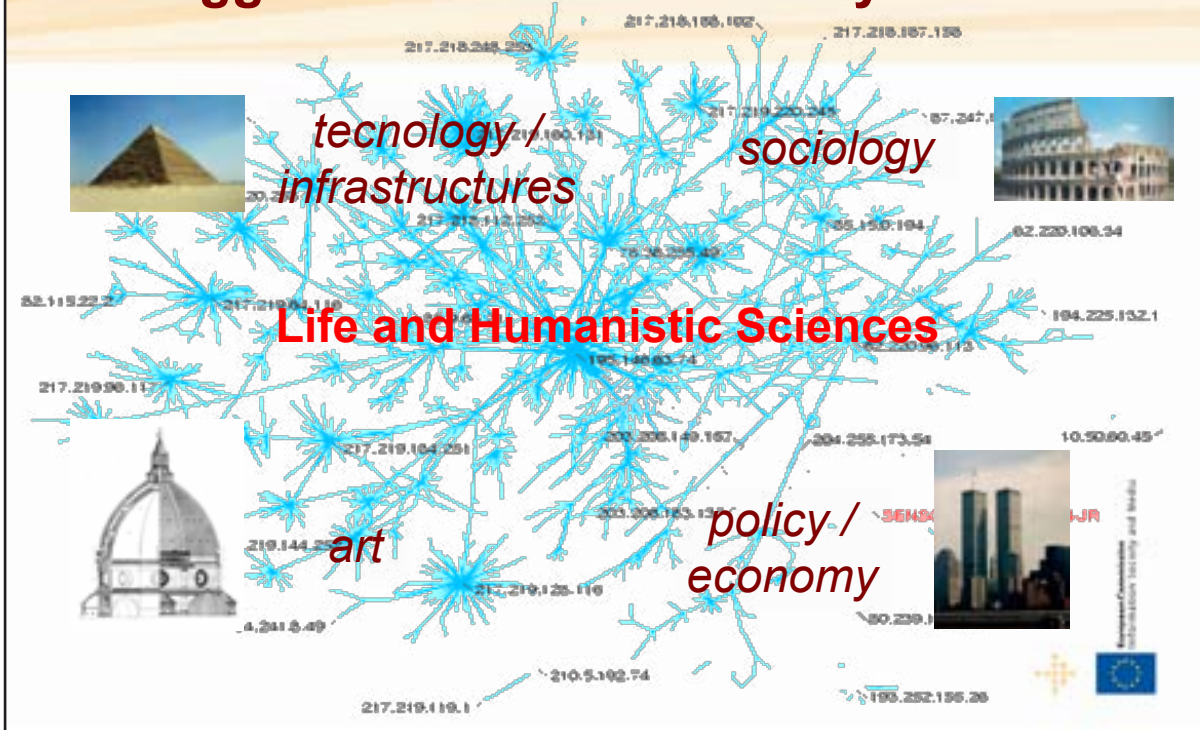


m

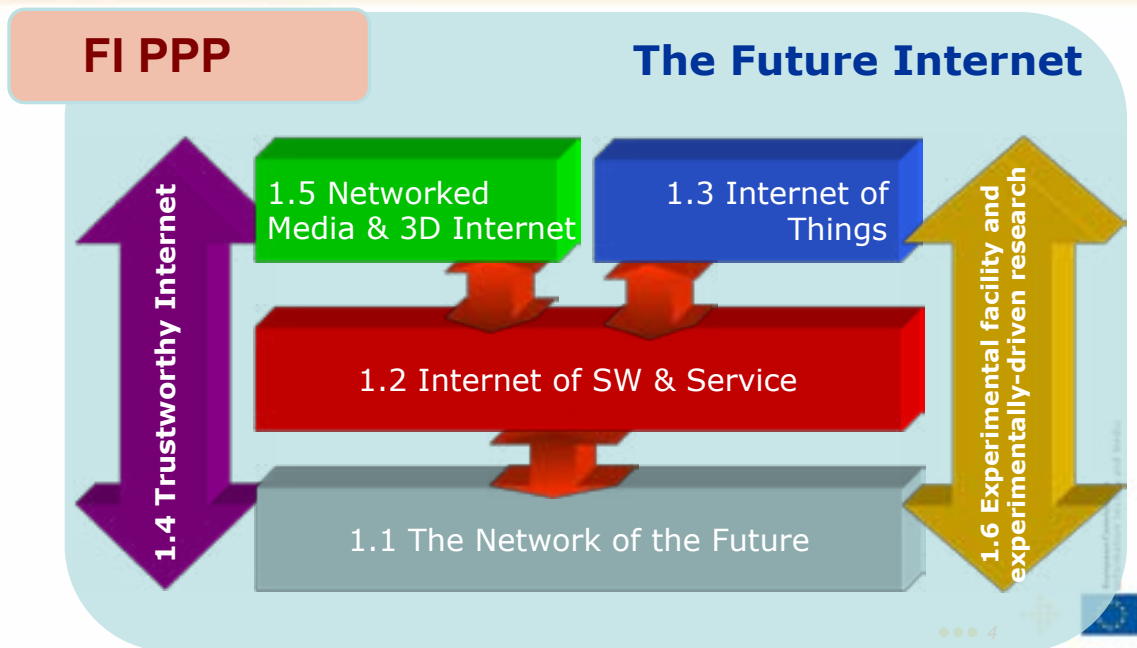
what is the biggest artefact ever built by mankind?



what is
the biggest artefact ever built by mankind?



EU ICT research 2006/2013 in Future Internet
Approx. budget: **2 billion euro**



Internet is not just about technology...

- **Economic transformation**

- Productivity gains in standard businesses
- New businesses/SMEs, new advertisement paradigms, energy grids
- New economic models (skype, google, apple, cloud, ...)



- **Social expansion**



- Ubiquitous access to information (copyrighted or free: wikipedias, googlemaps, ...)
- Online social networking (Linkedin, Facebook, Twitter, ...)
- Personal expression (Youtube, Flickr, ...)

- **Psychological change**

- Internet time (affecting workstyles and lifestyles)
- Globalisation, multilinguality, Augmented Reality
- Online Trust



- **Legal Impact**

- Redefinition of Privacy and Identity
- Copyrights in the digital era
- Cybercrime



••• 5



European Commission
Information Society and Media

two questions...

- **the present Internet: was it ...**



planned?



or just **serendipitous?**

- **the future Internet: what will it look like?**



••• 6



European Commission
Information Society and Media

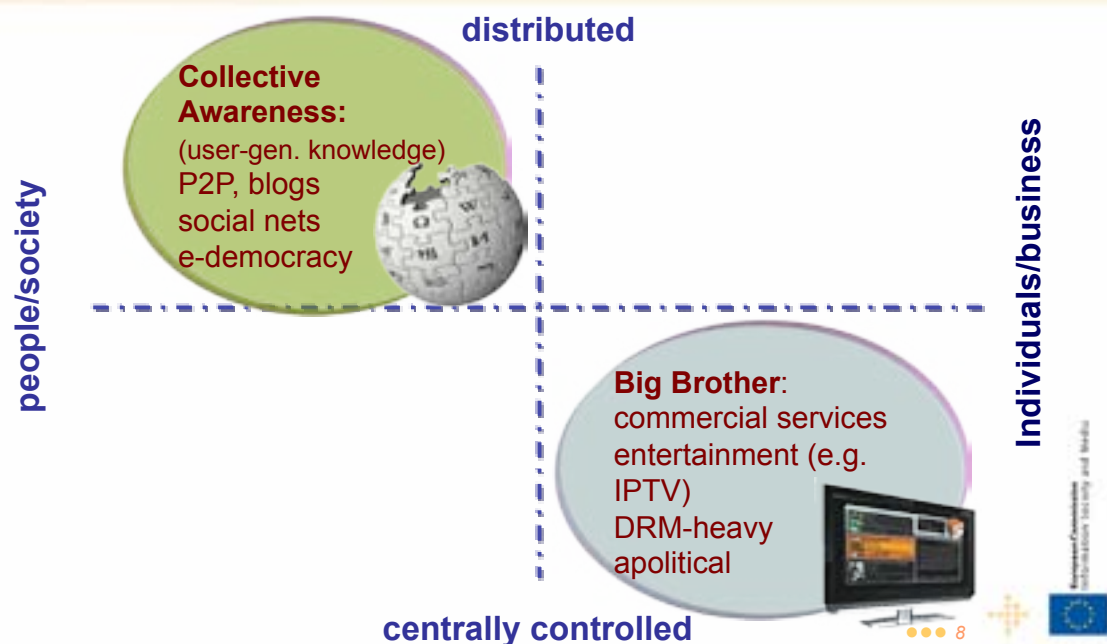
Future Internet & sustainability: an ethical question?

- We are facing the convergence of multiple crises
 - **Financial, Environmental, Energy, Social**
- How can Internet help the transition towards a more sustainable future?
 - **Environmental-friendly way of living**
 - Product ranking, Life footprint, efficiency
 - **Sustainable economic development**
 - Empowering people, new market models, new IPR
 - **Participative global governance**
 - Based on cooperation, sharing, low-cost access





Future Internet scenarios

(See also the Oxford Internet Institute Study on Technological, Social and Economic aspects of FI, <http://cordis.europa.eu/fp7/ict/fire/>)

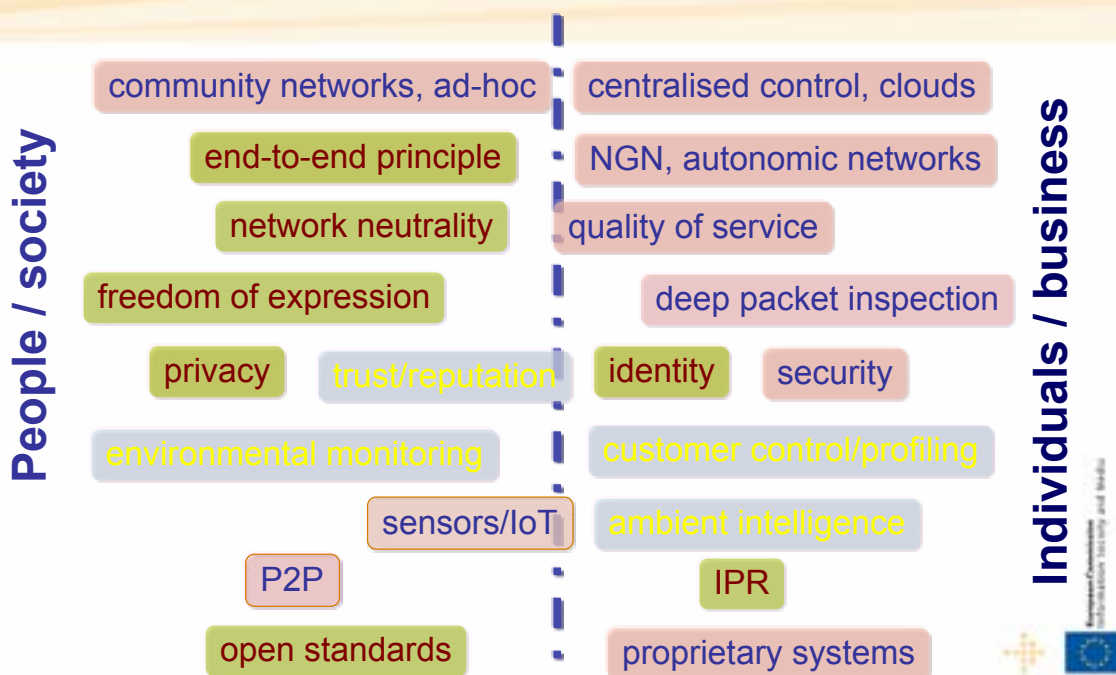


Technological and Policy choices have Social and Economic impacts

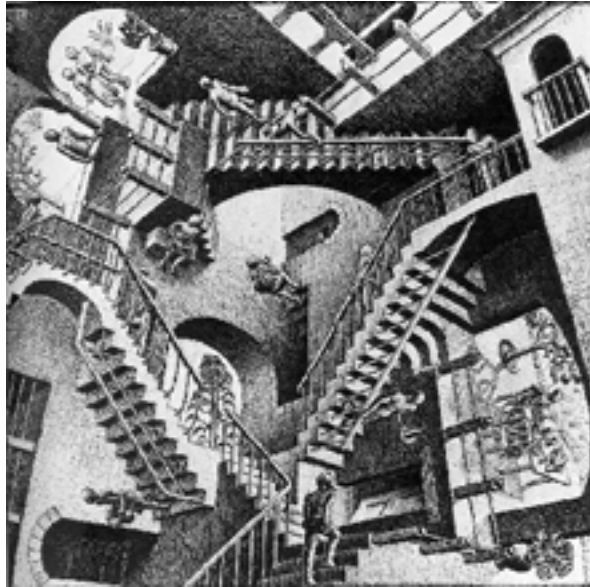
(OII Study, MIT workshop)

	Collective Awareness 	Big Brother 
Internet infrastructure	Current architecture ad hoc/mesh , user driven	Vertically integrated specialized nets
Technological developments	Interoperability Distributed control Generalized wiki	NGN or "clean slate" for streaming Walled gardens
Security and Privacy	Privacy / identity more than security Online Reputation	Strong Security , proprietary
Policy	Light / no IPR protection Transparency	Strong IPR protection
Standards	Open or Open source standards Multi-cultural support	Competing closed standards may prevail National customisation
Network Neutrality	Key , to enforce	Just a burden

ethical aspects of technological / application / policy choices



Thanks!





Ethical aspects of information and communication technologies



Chengetai MASANGO

Programme and Technology Manager,
UN Internet Governance Forum

Chengetai Masango is the Programme and Technology Manager at the United Nations Secretariat for the Internet Governance Forum. He was a speaker at Africa Electronic Privacy and Public Voice Symposium and holds both a PhD in information policy and an MA in international relations from Syracuse University.

Mr Masango conducted a study of the politics of the .zw top-level domain (TLD) and generic second-level domains (SLDs) under it (.org, .com etc.) as part of an independent study.

Publications

Encouraging Internet public policy development and capacity building in developing countries: Lessons from the FLOSS community and, as a co-author, *Internet governance and the information society: Global perspectives and European dimensions* and *Effective work practices for software engineering: free/libre open source software development*.

The UN Internet Governance Forum

Chengetai MASANGO

The Internet Governance Forum European Group on Ethics Roundtable on ICT 15 November 2011

Chengetai Masango
Secretariat of the Internet Governance Forum (IGF)
<http://www.intgovforum.org/>

IGF Background

- One of the major outcomes of the World Summit of the Information Society (WSIS)
- Geneva Phase 2003
- WGIG
- Tunis Phase 2005

2

Internet Governance (Definition WGIG)

- *Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*

3

Internet Governance Forum

- Paragraph 72 of the [Tunis Agenda](#)
- Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
- Mandate of the IGF was for 5 years
- Renewed in 2010 for a further 5 years

4

What is the IGF:

- A platform for multi-stakeholder policy dialogue.
- It is based on a ‘soft governance’ approach.
- IGF can shape public opinion and decision making.

5

Structure

Secretary General's
Special Advisor
for Internet Governance

Stakeholders

Secretariat
of the
Internet Governance Forum





The African Group
The Asian Group
The Eastern European Group
The Latin American and Caribbean States (GRULAC)
The Western European and Others Group (WEOG)

Multi-stakeholder nature of the IGF

- The Tunis Agenda states that the IGF in its working and function will be multilateral, multi-stakeholder, democratic and transparent. (Tunis Agenda, section 73)

IGF Annual Meetings

- Annual meeting of four days.
- Six meetings so far:
 - Athens, 2006;
 - Rio de Janeiro, 2007;
 - Hyderabad, 2008;
 - Sharm El Sheikh, 2009;
 - Vilnius, 2010;
 - Nairobi, 2011;
 - Baku, 2012;
 - Indonesia, 2013 (Bid)

9

Regional & National IGF Initiatives

- There are approximately 9 regional IGFs
 - LAC Regional IGF
 - Caribbean IGF
 - East Africa IGF
 - West Africa IGF
 - Central Africa IGF
 - EuroDIG
 - Commonwealth IGF
 - Asia Pacific IGF
 - Southern African IGF
- There are approximately 16 national IGFs
 - Kenya
 - Côte d'Ivoire
 - Finland
 - Germany
 - Sweden
 - Spain
 - Russia
 - USA
 - New Zealand

10

Internet Governance

(Definition WGIG)

- *Internet governance is the **development** and application by Governments, the private sector and civil society, in their respective roles, of **shared principles, norms, rules**, decision-making procedures, and programmes that shape the evolution and use of the Internet.*

11

Promoting Principles, Norms & Standards

- No universal standards or principles on ethics.
- Scope, definition
- Multistakeholder approach
- Provide a space for discussion
- Raise awareness of issues
- Dynamic Coalitions

Dynamic Coalitions

Dynamic Coalitions emerging from the workshops:

- Open Standards (Brazil, W3C, Sun..);
- Internet Rights and Principles (Brazil, ISOC Italy, IP Justice...);
- FOEonline (Freedom of Expression and the Media)
- Child online Safety (ECPAT, Save the Children, Childnet International)

13

More Information

www.intgovforum.org

igf@unog.ch

14



Ethical aspects of information and communication technologies

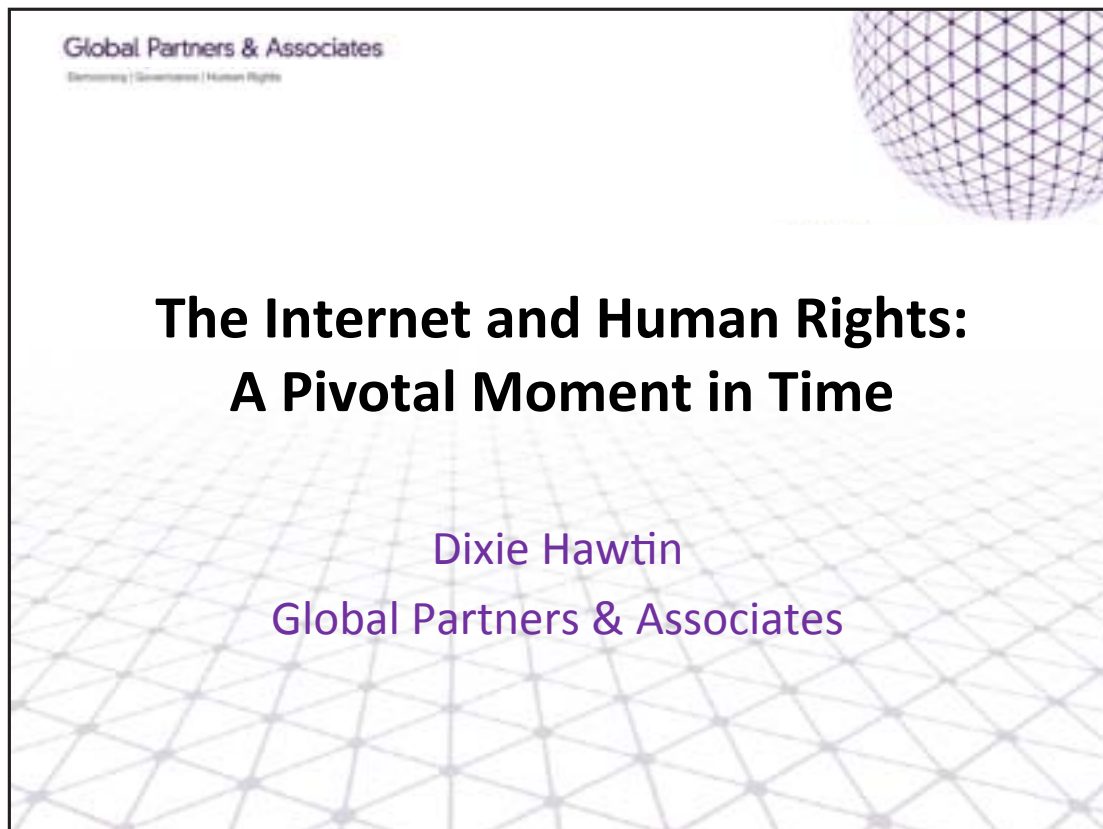


Dixie HAWTIN

Project Manager, Freedom of Expression,
Global Partners and Associates

Dixie Hawtin is Project Manager for Freedom of Expression and Digital Communications work at Global Partners and Associates. Her expertise lies in policy research, advocacy work and capacity building aimed at fostering a global digital communications environment that is open and empowering and that supports human rights. Current activities include: a major international study on the impact of the Internet and mobile phones

on the media and human rights sectors; a civil society capacity-building project in south Asia; and a project mapping global issues and regulatory responses to protecting privacy on the Internet. Dixie is also co-chair of the Dynamic Coalition on Internet Rights and Principles, an international multi-stakeholder network of individuals and organisations working to uphold human rights in and through Internet governance.



The Threats:

The Internet faces a challenge from both public power and private power, and sometimes a deadly combination of the two.

- **Governments** – illegitimate reasons
- **Governments** – legitimate reasons
- **Businesses** – commercial priorities

Three values:

- A **GLOBAL PUBLIC VALUE SPACE**
- A **MULTI-STAKEHOLDER** approach
- **HUMAN RIGHTS** as driving principles





Addressing the PROCESS crisis:

Invest in global multi-stakeholder processes



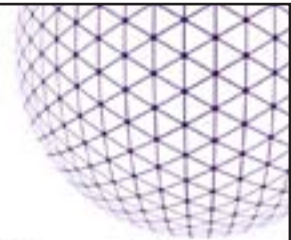
Addressing the POLICY crisis:

Invest in building a positive normative framework



A major cross-cutting issues:
Put copyright in its place

Global Partners & Associates
Democracy | Governance | Human Rights



Questions?

Thank you



Ethical aspects of information and communication technologies



William ECHIKSON

External Relations, Communications and Public Affairs, Head of Free Expression EMEA at Google

William Echikson is Head of Free Expression Policy and PR, Europe, Middle East and Africa for Google. He is a veteran Europe correspondent, who has written for a series of prestigious US publications including the *Christian Science Monitor*, *Wall Street Journal*, *Fortune* and *BusinessWeek* over the past 25 years. From 1985 to 1990, he covered the collapse of communism in central Europe, publishing a book *Lighting the night: Revolution in eastern Europe* containing his observations and experiences. He turned to business and cultural reporting in the 1990s, and published two more books, *Burgundy stars*, a behind-the-scenes look at a French gastronomic shrine, and *Noble rot*, on the Bordeaux wine world. From 2001 to 2007, he managed the Brussels bureau for Dow Jones as

bureau chief. He has considerable experience with EU issues, most prominently antitrust, trade and environment.

William has other interesting journalistic experience. He worked for a European newspaper, serving as editor-in-chief of *Libération's* special international supplements during the mid-1990s. He also has written, directed and produced television documentaries for America's Public Broadcasting Service. William joined Google in 2008 as the company's Brussels spokesman. He became responsible for communications in southern and eastern Europe, the Middle East and Africa the following year and now focuses on free expression throughout Europe, the Middle East and Africa.

Internet governance, Google perspective

William ECHIKSON



UGC is fuelling web growth



UGC is fuelling web growth



UGC is fuelling web growth



UGC is fuelling web growth



UGC is fuelling web growth



UGC is fuelling web growth



Web is a powerful force for societal transformation



Technology is a double-edged sword



Example: Iran



Growing threat of Internet censorship



Growing threat of Internet censorship

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas **through any media** and **regardless of frontiers**”

– Article 19, 1948 Universal Declaration of Human Rights

Google supports free expression – within limits



Google's default position is to let information flow



We seek to be transparent about government requests



Example: Transparency report



Example: Web traffic visualisation



Example: Speak2Tweet in Egypt



Promoting trade benefits of an open internet



The Global Network Initiative



European political support for freedom of expression



European political support for freedom of expression

“When you set people free you set the conditions for society and the economy to develop... The **most important instrument of change in our time is the Internet**”

– Swedish Foreign Minister, Carl Bildt

European political support for freedom of expression

“Respect for media pluralism, protection of journalists’ sources, freedom to criticise private and government powers... are all essential for the full exercise of freedom of expression, and the **Commission is fully committed to the defence of fundamental rights**”

– Vice President of the European Commission, Neelie Kroes

European political support for freedom of expression



Battling online censorship needs sustained cooperation







Ethical aspects of information and communication technologies



Peter HUSTINX

European Data Protection Supervisor

Mr Hustinx has been European Data Protection Supervisor since January 2004 and was reappointed by the European Parliament and the Council in January 2009 for a second term of five years. He has been closely involved in the development of data protection law from the start, at both national and international levels.

Before entering office, Mr Hustinx was President of the Dutch Data Protection Authority since 1991. From 1996 to 2000, he was Chairman of the Article 29 Working Party.

He has law degrees from universities in Nijmegen, the Netherlands, and Ann Arbor, USA. Since 1986 he has been a deputy judge in the Court of Appeal in Amsterdam.

Data protection in an Internet-driven society

Peter HUSTINX



Opinion of the European Data Protection Supervisor

on net neutrality, traffic management and the protection of privacy and personal data

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data², and in particular Article 41(2) thereof,

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector³,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1. Background

1. On 19 April 2011, the Commission adopted a Communication on the open internet and net neutrality in Europe⁴.
2. This Opinion can be seen as the reaction of the EDPS to this Communication and aims at contributing to the ongoing policy debate within the EU on net neutrality, especially on aspects related to data protection and privacy.

¹ OJ L 281/31, 23.11.95, pp. 31–50, the ‘Data Protection Directive’.

² OJ L 8, 12.1.2001, p. 1, the ‘Data Protection Regulation’.

³ OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (see footnote 15), the ‘ePrivacy Directive’.

⁴ COM(2011) 222 final.

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 63

E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu

Tel.: 02-283 19 00 - Fax : 02-283 19 50

3. The Opinion builds on the answer⁵ of the EDPS to the Commission's public consultation on The Open internet and net neutrality in Europe, which preceded the Commission's Communication. The EDPS has also taken note of the recent draft Council conclusions on net neutrality⁶.

I.2. The concept of net neutrality

4. Net neutrality refers to an ongoing debate on whether Internet service providers (ISPs⁷) should be allowed to limit, filter, or block Internet access or otherwise affect its performance. The concept of net neutrality builds on the view that information on the Internet should be transmitted impartially, without regard to content, destination or source, and that users should be able to decide what applications, services and hardware they want to use. This means that ISPs cannot, at their own choice, prioritise or slow down access to certain applications or services such as Peer to Peer ('P2P'), etc⁸.
5. Filtering, blocking and inspecting network traffic raises important questions, often overlooked or sidelined, regarding the confidentiality of communications and the respect for the privacy of individuals and their personal data when they use the Internet. For instance, certain inspection techniques involve the monitoring of content of communications, websites visited, emails sent and received, the time when this takes place, etc, enabling filtering of communications.
6. By inspecting communications data, ISPs may breach the confidentiality of communications, which is a fundamental right, guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the 'ECHR') and Article 7 and 8 of the Charter of Fundamental Rights of the European Union (the 'Charter'). Confidentiality is further protected in secondary EU legislation, namely Article 5 of the ePrivacy Directive.

I.3. Focus and structure of the Opinion

7. The EDPS considers that a serious policy debate on net neutrality must address the confidentiality of communications as well as other privacy and data protection implications.
8. This Opinion contributes to this ongoing EU debate. Its goal is threefold:
 - It flags the relevance of privacy and data protection in the current discussions on net neutrality. More particularly, it highlights the need to respect the existing rules on confidentiality of communications. Only practices that respect such rules should be allowed.

⁵ EDPS responded stressing the importance of taking into account data protection and privacy issues together with other existing rights and values. The response is available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf.

⁶ Available at <http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf>.

⁷ This includes the provision of both fixed and mobile access to the Internet.

⁸ Although the principle does apply to ISPs putting limits on the speed or amount of information a subscriber is able to send or receive through subscriptions with bandwidth or volume limits. Therefore, under a net neutrality principle ISPs would still be able to offer Internet access subscriptions limiting access based on criteria such as speed or volume as long as it does not require discriminating in favour or against particular content.

- Net neutrality relates to relatively new - technological - possibilities and there is little experience on how the legal framework applies. This Opinion therefore provides guidance on how ISPs must apply and respect the data protection legal framework if they engage in filtering, blocking and inspecting network traffic. This should be helpful for ISPs and also for authorities in charge of enforcing the framework.
 - Within the scope of data protection and privacy, this Opinion identifies areas which call for special attention and which may require action at EU level. This is particularly important in the light of the ongoing debate at EU level and the policy measures that may be launched by the Commission in this context.
9. The EDPS is aware that net neutrality raises other issues, further described below, such as those related to access to information. These issues are only addressed to the extent that they are related to or have an impact on data protection and privacy.
10. The Opinion is structured as follows. Section II starts by providing a short overview of practices on filtering by ISPs. Section III outlines the EU legal framework on net neutrality. Section IV continues with a technical description followed by an assessment of the privacy implications, depending on the technique used. Section V analyses the practical details regarding the application of the current EU privacy and data protection framework. Building on the analysis, Section VI contains suggestions for further policy developments and identifies the areas where clarification and improvement of the legal framework might be needed. Section VII contains the conclusions.

II. NET NEUTRALITY AND TRAFFIC MANAGEMENT POLICIES

Increasing use of traffic management policies

11. Traditionally, ISPs have engaged in monitoring and influencing network traffic only in limited circumstances. For example, ISPs have applied inspection techniques and restricted information flows to preserve the security of the network, e.g. to fight viruses. Therefore, generally speaking, the Internet has grown while preserving a great degree of neutrality.
12. However, in recent years, some ISPs have shown an interest in inspecting network traffic in order to differentiate and apply different policies to it, for example, to block specific services or give preference access to others. This is sometimes referred to as ‘traffic management policies’⁹.
13. The reasons for ISPs to inspect and differentiate traffic are manifold. For example, traffic management policies may help ISPs to manage traffic during periods of high congestion, for example, by prioritising certain time-sensitive traffic, such as video streaming and downgrading other types of traffic which may be less time sensitive,

⁹ See for example, OFCOM Report entitled ‘Site blocking to reduce online copyright infringement’, adopted on 27 May 2011, available at: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-report_with_redactions_vs2.pdf: ‘Some ISPs already deploy packet inspection systems in their network for traffic management and other purposes, so we assume that it can be deployed, albeit that this would involve a high level of complexity and cost for those not already running such services. It may be that in the short to medium term DPI could only be deployed by the larger ISPs given the capital investment required’.

such as P2P¹⁰. Furthermore, traffic management may be a means for ISPs to obtain a potential revenue stream, which could originate from different sources. On the one hand, ISPs could charge fees to content service providers, for example, those whose services require using higher bandwidth, in exchange of giving them priority (and thus speed). This would mean that accessing a certain service, for example, a service providing videos on demand, would be faster than accessing another similar service which has not signed up to high speed transmission. Revenues could also be obtained from subscribers interested in paying higher (or lower) fees for certain types of differentiated subscriptions. For example, a subscription without access to P2P could be cheaper than one giving unlimited access.

14. In addition to the ISP's own reasons for the use of traffic management policies, other parties may also have an interest in ISP's using traffic management policies. If ISPs manage their networks and engage in inspection of content which goes through their facilities, they are likely to increase their capacity to detect alleged unlawful usage, e.g. breach of copyright or pornographic use.

Other interests at stake, including data protection and privacy

15. This trend has triggered a debate on the legitimacy of this type of practices and more particularly whether specific net neutrality obligations should be further developed by law.
16. Increasing use by ISPs of traffic management policies could possibly limit access to information. If this behaviour became common practice and it was not possible (or highly expensive) for users to have access to the full Internet as we know it, this would jeopardise access to information and user's ability to send and receive the content they want using the applications or services of their choice. A legally mandatory principle on net neutrality may avoid this problem.
17. This brings the EDPS to the implications for data protection and privacy when ISPs engage in traffic management. More particularly:
 - When ISPs process traffic data with the sole purpose of routing the information flow from the sender to the receiver, they generally carry out limited personal data processing¹¹. In the same way as the postal service processes the information included on the envelope of a letter, the ISP processes the information needed to route the communication towards the recipient. This does not conflict with the legal requirements of data protection, privacy and confidentiality of communications.
 - However, when ISPs inspect communication data in order to differentiate each communication flow and to apply specific policies, which may be unfavourable to individuals, the implications are more significant. Depending on the circumstances of each case and on the type of analysis performed, the processing may be highly intrusive for an individual's privacy

10 The quality of real-time applications such as video streaming is, among other things, dependent on latency, i.e., delay due for example to network congestion.

11 This excludes operations aimed at increasing the security of the network and detecting harmful traffic and also operations required for billing and interconnection. It also excludes obligations that derive from the Data Retention Directive, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006, L 105/54 ('Data Retention Directive').

and personal data. This is more obvious where management policies reveal the content of individuals' Internet communications, including emails sent and received, websites visited, files downloaded or uploaded, etc.

III. OVERVIEW OF THE EU LEGAL FRAMEWORK ON NET NEUTRALITY AND FURTHER POLICY DEVELOPMENTS

III.1. The legal framework in a nutshell

18. Until 2009, EU legislative instruments did not contain provisions explicitly prohibiting ISPs from engaging in filtering or blocking or charging extra costs to subscribers for access to services. At the same time, they did not contain provisions explicitly recognising this practice. The situation was, to some extent, one of uncertainty.
19. The 2009 Telecom package changed this by including provisions favouring the openness of the Internet. For example, Article 8(4) on a common regulatory framework for electronic communications networks and services ('Framework Directive') establishes an obligation on regulatory authorities to promote the ability of end users to access content, applications or services of their choice¹². This provision applies to the network as a whole, not at the level of individual providers. Recent draft Council conclusions also highlighted the need to maintain the openness of the Internet¹³.
20. The Universal Service Directive¹⁴ contains more concrete obligations. Articles 20 and 21 set forth transparency requirements regarding limitations on access to and/or use of services and applications. It also requires minimum service quality levels.
21. For ISP practices entailing the inspection of individuals' communications, Recital 28 of the Directive amending the Universal Service and ePrivacy Directives¹⁵ highlights that 'depending on the technology used and the type of

¹² Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services, as amended by Directive 2009/140/EC and Regulation 544/2009, OJ 337, 18.12.2009, p. 37.

¹³ See point 3(e), where Council recognises: 'The need to maintain the openness of Internet while ensuring that it can continue to provide high-quality services in a framework that promotes and respects fundamental rights such as freedom of expression and freedom to conduct business' and 8(d), inviting Member States to 'Promote the open and neutral character of the Internet as their policy objective'.

¹⁴ Directive 2002/22/EC as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. OJ L 337/11, 18.12.2009. Compare also Article 1(3), stating that the Directive neither mandates nor prohibits ISPs from limiting end-users' access to, and/or use of, services and applications, where allowed under national law and in conformity with Community law, but requires them to inform about any such conditions.

¹⁵ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. OJ L 337/11, 18.12.2009.

limitation, such limitation may require user consent under the ePrivacy Directive'. Thus, Recital 28 recalls the need for consent pursuant to Article 5(1) of the ePrivacy Directive for any limitations based on monitoring of communications. Section IV below further analyses the application of Article 5(1) and the overall data protection and privacy legal framework.

22. Finally, Article 22(3) of the Universal Service Directive now empowers national regulatory authorities to impose, if necessary, minimum quality of service requirements on ISPs in order to prevent the degradation of services and the hindering or slowing down of traffic over public networks.
23. The above means that at the EU level there is a broad aspiration to an open Internet (see Article 8(4) of the Framework Directive). However, this policy objective, which applies to the network as a whole, is not directly linked to prohibitions or obligations on individual ISPs. In other words, an ISP could engage in traffic management policies, which may exclude access to certain applications, provided that end-users are fully informed, and have expressed their consent freely, specifically and unambiguously.
24. The situation may differ depending on Member States. In some Member States ISPs can, under specific conditions, engage in traffic management policies, for example, to block applications such as VoIP (as part of a cheaper Internet subscription), provided that individuals have given their free, specific and unambiguous, informed consent. Other Member States have chosen to strengthen the principle of net neutrality. For instance, in July 2011 the Dutch Parliament passed a law generally prohibiting providers from hindering or slowing down applications or services on the internet (such as VoIP), unless necessary to minimise the effects of congestion, for integrity or security reasons, to fight spam or in accordance with a court order.¹⁶

III.2. The Communication on Net Neutrality

25. In its Communication on net neutrality¹⁷, the European Commission concluded that the situation on net neutrality is one that requires monitoring and further analysis. Its policy has been dubbed as 'wait and see', before considering further regulatory steps.
26. The Commission's Communication recognised that any measure and further regulatory steps would be subject to an in-depth assessment of data protection and privacy aspects. The draft Council conclusions also note the data protection and privacy issues at stake.¹⁸
27. The question to be assessed from a data protection and privacy perspective is whether a wait and see policy is sufficient. While the data protection and privacy framework does, at the present time, foresee some safeguards especially through

¹⁶ The original Dutch amendment can be found at: <https://zoek.officielebekendmakingen.nl/kst-32549-A.html>. The reasons reported by the press for such a policy option did not refer to data protection and privacy considerations but rather to reasons related to ensuring that users are not deprived of or offered limited access to information. So it seems that issues relating to access to information motivated this amendment.

¹⁷ See footnote 4.

¹⁸ See point 4(e), where Council notes: 'The existence of some concerns, mainly emerging from consumers and data protection authorities, in regard to personal data protection'.

the principle of confidentiality of communications, it appears necessary to monitor closely the level of compliance and issue guidance on several aspects that are not particularly clear. In addition, some thoughts should be put forward as to how the framework could be clarified and further improved, in the light of technological developments. If the monitoring reveals that the market is evolving towards massive, real-time inspection of communications and issues related to complying with the framework, legislative measures will be necessary. Concrete suggestions will be made in that respect in Section VI.

IV. TECHNICAL BACKGROUND AND RELATED PRIVACY AND DATA PROTECTION IMPLICATIONS

28. Before going more deeply into the subject, it is important to have a better view of the inspection techniques that may be used by ISPs to engage in traffic management and how this may impact the principle of net neutrality. The privacy and data protection implications derived from such techniques vary substantially depending on which technique/s is or are used. This technical background is necessary to understand and apply properly the legal data protection framework described in Section V. However, it should be noted that this is a constantly changing and complex area. The description below therefore is not intended to be exhaustive and fully up-to-date, but only to provide the technical information that is indispensable for understanding the legal reasoning.

IV.1. Transmission of information through the Internet: the basics

29. When a user transmits a communication via Internet, the information transmitted is divided into packets. These packets are transmitted across the Internet from the sender to the recipient. Each packet will include, among others, information about the source and the destination. In addition, ISPs might enclose these packets into additional layers and protocols¹⁹, which will be used to manage the different traffic flows within the ISP network.

30. To refer back to the analogy of the postal letter, using a network transmission protocol is equivalent to including the content of a postal letter into an envelope with a destination address to be read by the postal service and then having the postal service deliver it. The postal service may use additional protocols in its internal transits to manage all the envelopes to be transmitted, the goal being that each envelope reaches its destination as originally drafted by the sender. Using this analogy, each packet has two parts, the *IP payload* that includes the content of the communication and will be the equivalent to the letter. It contains information addressed only to the recipient. The second part of the packet is the *IP header* that includes, among others, the address of the recipient and the sender and will be the equivalent to the envelope. The IP header allows the ISPs and other intermediaries to route the payload from its source address to its destination address.

31. ISPs and other intermediaries ensure that IP packets travel across the network through nodes that read the IP header information, check it versus routing tables, and then forward them towards the next node in the path to the destination. This

¹⁹ As further described in Section IV.2, such protocols code the information being transmitted end-to-end in an agreed way so that the parties involved in the communication can understand each other, such as HTTP, FTP, etc.

process is done across the network using a ‘best effort memoryless’ approach since all the packets arriving to a node are treated in a neutral way. When they have been forwarded to the next node, there is no need to retain further information in the router²⁰.

IV.2. Inspection techniques

32. As illustrated above, ISPs read IP headers for the purpose of routing them towards their destination. However, as outlined above, the analysis of traffic (involving IP headers and IP payloads) can be performed for other purposes and with different types of technologies. New trends may include for instance slowing down certain applications being used by users, such as P2P, or alternatively, enhancing traffic speed for certain services like video-on-demand services for premium subscribers. While all inspection techniques *technically* perform packet inspection, they involve different levels of intrusiveness. There are two main categories of inspection techniques. One is based on just the IP header, the other also on the IP payload.

- *Based on the IP header information.* The inspection of an IP packet header reveals some fields that may allow ISPs to apply a number of specific policies to manage the traffic. These techniques based only on inspection of IP headers process data which, in principle, is meant for routing information, for a different purpose (i.e. differentiating traffic). Looking at the source IP address, the ISP can link it to a concrete subscriber and apply some specific policies, for instance routing the packet through a faster or a slower link. Looking at the destination IP address, the ISP can also apply specific policies, for instance blocking or filtering access to certain websites.

- *Based on a deeper inspection.* Deep packet inspection enables the ISP to access information addressed to the recipient of the communication only. Going back to the postal service example, this approach is equivalent to opening the envelope and reading the letter inside to perform an analysis of the content of the communication (encapsulated inside the IP packets) in order to apply a specific network policy. There are different ways of carrying out the inspection, each presenting different threats to the data subject.

- *Deep packet inspection based on the analysis of protocols and on statistical records.* In addition to the IP protocol, which is meant to enable the data to be transmitted across the Internet, there are additional protocols that code the information being transmitted in an agreed way (transport, session, presentation and application, etc.). The goal of these protocols is to ensure that the parties involved in the communication can understand each other. For instance, there are some protocols that are associated with web browsing²¹, others are for file transfer²², etc. Therefore inspection techniques based on the inspection of protocols and combined with statistical analysis aim at looking for specific patterns or

²⁰ Nevertheless, Internet network equipment uses routing protocols that will log activity, process traffic statistics, and exchange information with other network equipment in order to route IP packets using the most efficient path. For instance, when a link is congested or broken, and a router receives this information, it will update its routing table with some alternative not using that link. It is also worth noting the collection and processing that in some cases may be done for billing purposes or even in accordance with the requirements of the Data Retention Directive.

²¹ HTTP - Hypertext transfer protocol - or HTML - Hypertext Markup Language.

²² FTP - File transfer protocol.

fingerprints that determine which protocols are present²³. These inspection techniques enable the ISPs to understand the type of communication (email, web browsing, uploading files) and, in some cases, to identify the specific service or application used, such as the case of some VoIP communications where the protocols used are very specific to a concrete vendor or service provider. The knowledge of the type of communication by itself can allow ISPs to apply concrete traffic management policies. For example, to block web traffic. It may also be the first step in allowing the ISP to perform further analyses that might require full access to the metadata and content of the communication.

- *Deep packet inspection based on the analysis of the content of the communication.* Finally, it is also possible to inspect the metadata²⁴ and the content of a communication itself. This technique consists in the interception of all the IP packets that are part of the original communication flow so that the original content of the communication can be reconstructed in full and analysed. For example, to detect harmful or illegal content like viruses, child pornography, etc, it is necessary to reconstruct the content itself so that it can be analysed. It is to be noted that sometimes the communication can be explicitly encrypted end-to-end by the parties involved and this practice will impede ISPs to perform analysis of the content of the communication.

IV.3. Privacy and data protection implications

33. Inspection techniques based on IP headers and more particularly those based on packet inspection involve the monitoring and filtering of these data and have serious implications in terms of privacy and data protection. They can also be in conflict with the right to confidentiality of communications.
34. Looking into individuals' communications has, in itself, serious privacy and data protection implications. Yet, the problem is broader since, depending on the effects pursued with the monitoring and interception, the privacy implications may further increase. Indeed, it is not the same to merely inspect communications, for example, to ensure that the system works well, and to inspect communications to apply policies which may have an impact on individuals. When traffic and selection policies may seek to avoid network congestion only, there will usually be no major implications for individual's privacy. However, traffic management policies may seek to block some content information, or influence the communication for instance through behavioural advertising. In those cases the effects are more intrusive. The concern becomes more critical if one realises that this type of information would be collected not for a small group of individuals but rather on a generalised basis, for all ISP customers²⁵. If all ISPs embrace filtering techniques,

²³ There are different ways of identifying the protocols used. For example, it is possible to search in specific fields in inner protocols, e.g. to identify ports used to establish the communication. A statistical characterization of a communication flow can also be inferred from the analysis of some specific fields, correlation of the protocols used simultaneously between two IP addresses.

²⁴ Each protocol has some specific fields in its header that provide additional informal information about the communication being transmitted. Therefore the content of those fields can be referred to as the metadata of the communication. An example of these fields can be the port number used, where, for instance if it is number 80, it is quite likely that the type of communication is web browsing.

²⁵ Of course, tracking capabilities are not exclusive to ISPs. Instead, ad. network providers are also capable, through the use of third party cookies to track users across websites. See for example a recent

this could lead to a generalised monitoring of Internet usage. Furthermore, if one focuses on the type of information being processed, the risks to privacy are obviously high, as much of the information being collected is likely to be very sensitive and, after collection, is available to ISPs and to those who would seek information from them. Furthermore, the information might also be very valuable in commercial terms. In itself, this represents a high risk of function creep where the initial purposes could easily evolve into commercial or other exploitation of the information collected.

35. The correct application of monitoring and inspection and filtering techniques must be done in conformity with the applicable data protection and privacy safeguards, which lay down limits as to what can be done and under which circumstances. Next follows an overview of the applicable safeguards under the current EU data protection and privacy legal framework.

V. APPLICATION OF THE EU PRIVACY AND DATA PROTECTION LEGAL FRAMEWORK

36. The EU data protection framework is technologically neutral; as such, it does not regulate specific inspection techniques as those described above. The ePrivacy Directive regulates privacy in the provision of electronic communication services in public networks (typically Internet access and telephony)²⁶ and the Data Protection Directive regulates data processing in general. Taken as a whole this legal framework sets out different obligations that apply to ISPs that process and monitor traffic and communications data.

V.1. Legal grounds to process traffic and content data

37. Under data protection legislation, the processing of personal data, such as in this case the processing of traffic and communication data, requires an adequate legal ground. In addition to this general requirement, specific requirements may apply in certain cases.
38. In this case, the type of personal data that are processed by ISPs refers to the traffic data and content of communications. The content of communications and the traffic data are both protected by the right to confidentiality of correspondence, which is guaranteed by Article 8 ECHR and Article 7 and 8 of the Charter. More particularly, Article 5(1) of the ePrivacy Directive, entitled 'confidentiality of communications' requires Member States to ensure the confidentiality of

academic article showing that Google has a presence on 97 of the top 100 websites, which means that Google can track users who have not opted out of third party cookies as they browse these popular websites. See: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respanning (July 29, 2011). Available at SSRN: <http://ssrn.com/abstract=1898390>. The tracking of users through third party cookies has been addressed by the Article 29 Working Party. See Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010 (WP 171).

²⁶ Article 1.2 of the ePrivacy Directive reads: 'In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals'. Also, Recital 17 is relevant in relation to data subject consent: 'For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC'.

communications and the related traffic data by means of a public communications network and publicly available electronic communications services. At the same time, Article 5(1) of the ePrivacy Directive foresees that the processing of traffic and content data by ISPs may be allowed, in certain circumstances, with the consent of the users. This is done by setting forth a prohibition to the 'listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)'. This is further developed below.

39. In addition to the consent of users concerned, the ePrivacy Directive foresees other grounds that may legitimise ISPs' processing of traffic and communication data. The relevant legal grounds for processing in this case are (i) delivering the service; (ii) safeguarding the security of the service, and (iii) minimizing congestion. Other possible grounds to legitimise management policies based on traffic or communication data are discussed below under (iv).

(i) Legal grounds for delivering the service

40. As illustrated in Section IV, ISPs process the information on IP headers for purposes consisting in routing each IP packet towards its destination. Article 6(1) and Article 6(2) of the ePrivacy Directive allow processing of traffic data for the purposes of conveyance of a communication. Thus, ISPs may process the information that is necessary for the delivery of the service.

(ii) Legal grounds for safeguarding the security of the service

41. Pursuant to Article 4 of the ePrivacy Directive, an ISP is under a general obligation to take appropriate measures to safeguard security of its services. The practice of filtering viruses may involve the processing of IP headers and IP payload. Taking into account that Article 4 of the ePrivacy Directive requires ISPs to ensure the security of the network, this provision legitimises inspection techniques based on IP headers and content that aim strictly to achieve such purpose. In practice, this means that, within the limits set forth by the proportionality principle (see Section V.3), ISPs may engage in monitoring and filtering of communications data to fight viruses and overall ensure the security of the network.²⁷

(iii) Legal grounds for minimising the effects of congestion

42. The *rationale* for this legal ground is to be found in Recital 22 to the ePrivacy Directive, explaining the Article 5(1) prohibition on storage of communications. This does not prohibit any automatic, intermediate and transient storage in so far as it takes place for the sole purpose of carrying out the transmission and does not last longer than necessary for the transmission and traffic management purposes, and the confidentiality of the communications remains guaranteed.
43. If there is a congestion, the question arises whether ISPs may consider randomly dropping or delaying traffic or rather slowing communications that are not time-

²⁷ Article 29 Working Party's Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006 (WP 118). In this Opinion the Working Party considers that using filters for the purpose of Article 4 can be compatible with Article 5 of the ePrivacy Directive.

sensitive, e.g. P2P or email traffic, enabling, for example, voice traffic to pass at acceptable quality.

44. Given the overall societal interest of guaranteeing a usable communications network, ISPs may argue that prioritising or throttling traffic to address congestion is a legitimate measure which is necessary to deliver an adequate service. This means that in these cases and for this purpose, there would be a general legal ground for processing personal data and specific consent by users would not be necessary.
45. At the same time, the ability to interfere in this way is not unrestricted. If ISPs need to inspect communications, from the perspective of confidentiality, and applying strictly the proportionality principle, they must use the least intrusive method available to achieve the purpose (avoiding deep packet inspection), and they must only apply it for as long as necessary to resolve the congestion.

(iv) Legal grounds for processing data for other purposes

46. ISPs may also want to inspect traffic and content data for other purposes, for example offering targeted subscriptions (e.g. a subscription that limits access to P2P or a subscription that increases speed for certain applications). Inspection and further use of traffic and communication data for purposes other than delivering the service or ensuring its security and lack of congestion is only allowed under strict conditions, in compliance with the legal framework.
47. The legal framework is mainly Article 5(1) of the ePrivacy Directive which requires consent from users concerned to listen, tap, store or engage in other kinds of interception or surveillance of communications and the related traffic data. In practice this means that consent of users involved in a communication is necessary to legitimise the processing of both traffic and communications data pursuant to Article 5(1).
48. As explained above, the application of inspection and filtering techniques is either based on IP headers, which constitute traffic data, or based on deep packet inspection which also entails IP payloads and constitute communication data. Therefore, in principle, the application of such techniques for purposes other than the conveyance of the service or security would be forbidden unless a legitimate ground allows for the processing, such as consent (Article 5(1)). An example where Article 5(1) would apply is when an ISP decides to offer customers a reduced rate for Internet access in return for receiving behavioural advertising, using deep packet inspection, and thus communication data, in order to do so. Real, specific and informed consent is therefore necessary according to Article 5(1).
49. Furthermore, Article 6 of the ePrivacy Directive entitled 'traffic data' provides certain rules applying specifically to traffic data. More particularly it foresees the possibility for ISPs to process traffic data based on users' consent to receive value added services²⁸. This provision specifies the consent requirement foreseen in Article 5(1) when traffic data are at stake.

²⁸ Recital 18 of the Directive contains a list exemplifying value added services. Whether services to which traffic management policies apply could be interpreted as part of the list is not clear. Traffic management policies aiming at prioritising certain content could be understood as providing a quality of the service. For example, traffic management that entails merely the processing of IP headers and has as its objective

50. In practice, it may not always be easy to ascertain, for example, in which cases consent is necessary, and in which cases the security of the network may legitimise the processing, particularly if the purposes of the inspection techniques are twofold (for instance avoiding congestion and providing added value services). It should be emphasised that consent cannot be considered as an easy and systemic gateway to compliance with data protection principles.
51. There is little experience on the application of the framework and more particularly on the various aspects that have been outlined above. This is an area where further guidance is essential, as further developed in Section VI. Furthermore, there are additional, relevant aspects related to obtaining consent that also require special consideration. These are described below.

V. 2. Issues related to providing informed consent as a legal ground

52. The consent required under Articles 5 and 6 of the ePrivacy Directive has the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC.²⁹ According to Article 2(h) of the Data Protection Directive, 'the data subject's consent' shall mean '*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*'. Recently, the role of consent and the requirements for it to be valid have been addressed by the Article 29 Working Party in its Opinion 15/2011 on consent³⁰.
53. ISPs requiring consent to engage in inspection and filtering of traffic and content data must therefore ensure that consent is free and specified, and it must be a fully informed indication of the individual's wishes by which he signifies his agreement to personal data relating to him being processed. Recital 17 of the ePrivacy Directive re-affirms this '(...) Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website'. Below follow some practical examples of what it means in this context for consent to be free, specific and informed.

Consent: Free, specific and informed indication of wishes

54. *Free consent.* Users should not have to suffer constraints linking consent to the Internet subscription they want to sign up to.
55. Individuals' consent would not be freely given if they had to consent to the monitoring of their communication data in order to get access to a communication service. This would be even more true if *all* providers in a given market were to engage in traffic management for purposes that went beyond security of the network. The only option left would be not to subscribe to an Internet service at all. Given that the Internet has become an essential tool both for work and for leisure purposes, not subscribing to an Internet service does not constitute a valid

to offer premium-priced gaming services, where users' personal gaming traffic is prioritised through the network could be seen as a value added service. On the other hand, it is far from clear whether traffic management to throttle certain types of traffic, for example to downgrade P2P traffic could be deemed as such.

²⁹ See Recital 17 and Article 2(f) of the ePrivacy Directive.

³⁰ Adopted on 13 July 2011 (WP 187).

alternative. The result would be that the individuals would have no real choice, i.e. they would not be able to freely give consent³¹.

56. The EDPS considers that there is a clear need for the Commission and national authorities to monitor the market, particularly to ascertain whether this scenario - i.e. providers linking telecommunication services to communication monitoring - becomes mainstream. Providers should offer alternative services, including an Internet subscription not subject to traffic management, without imposing higher costs to individuals.
57. *Specific consent.* The need for consent to be specific requires, in this case, that ISPs seek consent for the monitoring of traffic and communications data in a clear and distinctive way. According to the Article 29 Working Party, '... to be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities. This means in other words that the context in which consent applies is limited.' Specific consent is not likely to be obtained if the consent for the inspection of traffic and communications data is 'bundled' with the overall consent to subscribe for the service. Instead, specificity calls for the use of targeted means to obtain consent, such as a specific consent form or a separate box clearly dedicated to the purpose of monitoring (rather than inserting the information in the general conditions of the contract and requiring signature of the contract as it stand).
58. *Informed consent.* For consent to be valid it must be informed. The need to provide adequate prior information derives not only from the ePrivacy and Data Protection Directives but also from Articles 20 and 21 of the Universal Service Directive, as amended by Directive 2009/136³². The need for information and consent was expressly confirmed in Recital 28 of Directive 2009/136: 'Users should in any case be fully informed of any limiting conditions imposed on the use of electronic communications services by the service and/or network provider. Such information should, at the option of the provider, specify the type of content, application or service concerned, individual applications or services, or both'. It then specifies that: 'Depending on the technology used and the type of limitation, such limitations may require user consent under Directive 2002/58/EC'
59. Given the complexity of these monitoring techniques, giving meaningful prior information is one of the main challenges to obtain valid consent. Consumers should be informed in a way that they are able to understand the information that is being processed, how it is being used and the impact on the user experience and the level of privacy invasion related to the techniques.
60. This means not only that the information itself must be clear and understandable to average users, but also that the information is given directly to individuals in a conspicuous way so that they cannot overlook it.

³¹ A similar case is PNR where it was discussed whether the consent of passengers to transfer the booking details to the US authorities was valid. The Working Party considered that passengers' consent cannot be given freely as the airlines are obliged to send the data before the flight departure, and passengers therefore have no real choice if they wish to fly; Opinion 6/2002 of the Article 29 Working Party on transmission of passenger manifest information and other data from airlines to the United States.

³² Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (see footnote 15).

61. *Indication of wishes.* Consent under the applicable legal framework also requires an affirmative action by the user to signify his/her agreement. Implied consent would not meet this standard. This also confirms the need to use dedicated means to obtain consent enabling the ISP to inspect traffic and communications data in the context of applying traffic management policies. In its recent opinion on consent, the Article 29 Working Party stressed the need for granularity in obtaining consent with regard to the different elements that constitute the data processing.
62. One could argue that if the parties involved in a communication do not want ISPs to intercept it in order to apply traffic management policies, they can always encrypt the communication. This approach can be considered as helpful in practical terms, however it requires some effort and technical knowledge and it cannot be deemed similar to a free, specific and informed consent. Also, the use of encryption techniques do not keep a communication fully confidential since the ISP at least will be able to access the IP header information in order to route the communication and it also will be in a position to apply statistical analysis.
63. According to Article 5(1) of the ePrivacy Directive, consent must be obtained from the users concerned. In many cases, the user will be the same person as the subscriber, which allows consent at the moment of subscription of the telecommunication service. In other cases, including those where more than one person may be involved, consent of the users concerned will need to be obtained separately. This may raise practical issues as developed below.

Consent of all the users concerned

64. Article 5(1) provides for user consent to legitimise the processing. Consent must be obtained from *all users* involved in a communication. The *rationale* behind this is that a communication usually concerns at least two individuals (the sender and the recipient). For example, if an ISP scans IP payloads which refer to an email, they are inspecting information that relates to both the sender and the receiver of the email.
65. When monitoring and intercepting traffic and communications (for example, some web traffic), it may suffice for ISPs to obtain the consent of the user, that is, the subscriber. This is because the other party to the communication, in this case, a website visited, may not be considered as a ‘user concerned’³³. However, the situation may be more complex when such monitoring involves inspecting the content of emails and thus, personal information of the email sender and recipient, who may not both have a contractual relationship with the same ISP. Indeed, in these cases, the ISP would be processing personal data (name, email address and potentially sensitive content data) of non-customers. From a practical perspective obtaining consent from such individuals may be more difficult, as it should be done on a case-by-case basis rather than at the occasion of the conclusion of the telecommunication service. Nor would it be realistic to assume that the subscriber’s consent was also given on behalf of other users, as may often be the case in private households.

³³ Notwithstanding those cases where the web traffic involves the transfer of personal information such as, for example, pictures of identifiable natural persons posted on a website. The processing of such information requires a legal basis, but would not be covered by Article 5(1) as those persons would not be ‘users concerned’.

66. In this context, the EDPS considers that ISPs should abide by existing legal requirements and implement policies which do not involve the monitoring and inspection of information. This is all the more essential with regard to communication services which involve third parties who are not able to consent to the monitoring, particularly with regard to emails sent and received (this does not apply when the purpose is based on security considerations).
67. At the same time, it should be noted that national law implementing Article 5(1) of the ePrivacy Directive may not always be satisfactory on this point, and that in general there seems rather to be a need for better guidance as to the requirements of the ePrivacy Directive in this context. The EDPS therefore invites the Commission to be more active in this respect and take an initiative which might benefit from the input from supervisory authorities assembled in the Article 29 Working Party and from other stakeholders. If necessary, a case should be brought before the Court of Justice in order to create full clarity about the meaning and the consequences of Article 5(1).

V.3. Proportionality - data minimisation principle

68. Article 6(c) of the Data Protection Directive lays down the proportionality principle³⁴, which applies to ISPs, as they are data controllers in the meaning of this directive, when they engage in monitoring and filtering.
69. Pursuant to that principle, personal data may be processed only insofar as they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. The application of this principle entails the need to make an assessment as to whether the means employed for the data processing and the types of personal data used are suitable and reasonably likely to achieve their objectives. If the conclusion is that more data is collected than necessary, then, the principle is not met.
70. The conformity with the proportionality principle of certain types of inspection technique must be assessed on a case by case basis. It is not possible to reach conclusions *in abstracto*. However, it is possible to point at various concrete aspects that should be evaluated in assessing compliance with the proportionality principle.
71. *The amount of information processed.* Surveillance of communications of ISP customers at the deepest possible levels will in most of the cases be excessive and illegal. The fact that this may be done by means that are not apparent to individuals and that it may be difficult for them to understand what is happening increases the impact on their privacy. ISPs should assess which less intrusive means may be available to achieve the result required. For example, can monitoring of IP headers achieve the result required, in place of engaging in deep packet inspection? Even when using deep packet inspection, the identification of only certain protocols may deliver the necessary information. The application of data protection safeguards, including pseudo-anonymization, may also be relevant. The outcome of the assessment must confirm that the data processing is proportional.

³⁴As outlined above, the Data Protection Directive applies to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the ePrivacy Directive.

72. *The effects of processing (directly linked to the purposes).* Proportionality may be lacking in cases where ISPs use traffic management policies excluding access to certain services without allowing a fair share of the resulting benefit to users in return.

73. It is important to recall that the proportionality principle continues to apply even if other mandatory legal requirements have been satisfied, including if an ISP has, for example, obtained consent from individuals to engage in content monitoring. This means that the data processing carried out through content monitoring may still be illegal if it violates the underlying fundamental principle of proportionality.

V.4. Security and organizational measures

74. Article 4 of the ePrivacy Directive explicitly requires ISPs to take technical and organizational measures to ensure (i) that personal data is only accessed by authorised personnel and for lawful purposes; (ii) protection of personal data from accidental or unlawful processing, and (iii) implementation of a security policy with respect to the processing of personal data. It also enables national competent authorities to perform audits on these measures.

75. In addition, pursuant to Article 4(3) and (2) of the ePrivacy Directive, ISPs are also obliged to notify respectively competent national authorities in the event of a data breach, as well as the individuals affected in case that the disclosure can have adverse consequences for them.

76. Processing personal information included in communications with the goal of applying traffic management policies can give ISPs access to data that is even more sensitive than traffic data.

77. Therefore, the security policies developed by ISPs should incorporate specific safeguards to ensure that the measures taken are adequate to these risks. At the same time, national competent authorities auditing these measures should be particularly demanding. Finally, it should be ensured that effective notification procedures are put in place to inform data subjects whose information has been compromised and who may thus be affected negatively.

VI. SUGGESTIONS FOR POLICY AND LEGISLATIVE MEASURES

78. Inspection techniques based on traffic data and inspection of IP payloads, i.e. the content of communications, may reveal users' Internet activity: websites visited and activities on those sites, use of P2P applications, files downloaded, emails sent and received, from whom, on what subject and in which terms, etc. ISPs may want to use this information to prioritise some communications, such as video on demand, over others. They may want to use it to identify viruses, or to build profiles in order to serve behavioural advertising. These actions interfere with the right to the confidentiality of communications.

79. Depending on the techniques used and on the specifics of the case, the privacy implications will increase. The deeper the interception and analysis of the information collected, the greater the conflict with the principle of confidentiality of communications. The purposes for which the monitoring takes place and the data protection safeguards that have been applied are also key elements to

determine the degree of intrusion into the privacy and personal data of individuals. Blocking and monitoring for purposes of fighting malware, with strict limitations on the retention and use of the data inspected, cannot be compared to situations where the information is logged to build individual profiles to serve behavioural ads.

80. In principle, the EDPS considers that the existing EU privacy and data protection framework, if properly interpreted, applied and enforced, would be appropriate to guarantee that the right to confidentiality is upheld and overall that the protection of the privacy and data protection of individuals is not jeopardised³⁵. ISPs should not use such mechanisms unless they have properly applied the legal framework. More particularly, the relevant elements of the framework that ISPs should consider and respect include the following:

- ISPs can apply traffic management policies intending to provide security of the service, delivering the service, including limiting congestion, pursuant to Article 4 and 6 of the ePrivacy Directive.
- ISPs need another specific legal ground, and possibly users' consent, to apply traffic management policies which entail processing of traffic and/or communication data for purposes other than the above. For example, users' informed consent is necessary to monitor and filter the communications of individuals for the purposes of limiting (or allowing) access to certain applications and services such as P2P or VoIP.
- Consent must be free, explicit and informed. It should be indicated through an affirmative action. These requirements put strong emphasis on the need to step up the efforts to ensure that individuals are properly informed, in a way that is direct, understandable and specific so that they can assess the effects of the practices and ultimately make an informed decision. Given the complexity of these techniques, giving meaningful prior information to users is one of the main challenges to obtain valid consent. Besides, there should be no detrimental consequences (including financial costs) towards users who do not consent to any monitoring.
- The proportionality principle plays a crucial role when ISPs engage in traffic management policies, whatever the legal ground for processing and the purpose: delivering the service, avoiding congestion or providing targeted subscriptions with or without access to certain services and applications. This principle limits ISPs ability to engage in monitoring of the content of individual's communications that entail processing of excessive information or accruing benefits for ISPs only. What can logistically be performed by ISPs will depend on the level of intrusion of the techniques, the results required (for which they may accrue benefits) and the specific privacy and data protection safeguards applied. Prior to deploying inspection techniques, ISPs must engage in an assessment of whether these comply with the proportionality principle.

³⁵ This is without prejudice to the need for changes in the law based on other considerations, particularly in the context of the general review of the EU legal framework for data protection, with a view to making it more effective in the light of new technologies and globalisation.

81. While currently the legal framework includes relevant conditions and safeguards, there is a need to pay particular attention as to whether ISPs effectively meet the legal requirements, whether they provide the necessary information for consumers to make meaningful choices, and whether they observe the proportionality principle. At national level, the authorities competent for the above include the national telecommunication authorities on the one hand, and on the other, national data protection authorities. At EU level, relevant EU-level bodies include BEREC. The EDPS may also be able to play a role in this context.
82. In addition to monitoring the present level of compliance, given the relative novelty of the possibility of massive, real-time inspection of communications, some aspects related to the application of the framework that have been discussed in this Opinion require further more in-depth analysis and ulterior clarification. Guidance particularly relevant in several areas includes:
- Determining the inspection practices that are legitimate to ensure the smooth flow of traffic which may not require users' consent, such as, for example, the fight against spam. In addition to the intrusiveness of the monitoring applied, aspects such as, for example, the level of disturbance to the smooth flow of traffic that would otherwise occur, are relevant.
 - Determining which inspection techniques can be carried out for security purposes, which may not require users' consent.
 - Determining when monitoring requires individual's consent, notably the consent of all the users concerned, and the permissible technical parameters to ensure that the inspection technique does not entail processing of data that is not proportionate vis-à-vis its intended purposes.
 - Furthermore in the three cases above, guidance may be needed regarding the application of the necessary data protection safeguards (purpose limitation, security, etc).
83. Given that the competences in this field are both national and EU, the EDPS considers that sharing views and experiences in order to find harmonised approaches to the above is essential. To achieve that, the EDPS suggest the creation of a platform or an expert group which should gather together representatives of national regulatory authorities, the Article 29 Working Party, the EDPS and BEREC. The first goal of this platform would be to develop guidance, at least on the items identified above, in order to ensure solid and harmonised approaches and the same playing field. The EDPS calls upon the Commission to organise this initiative.
84. Last but not least, both national authorities as well as their EU counterparts, including BEREC and the EU Commission must pay close attention to market developments in this field. From a data protection and privacy perspective, the scenario where ISPs engage on a routine basis in traffic management policies offering subscriptions based on filtering access to content and applications, would be highly problematic. If this were ever to happen, legislation would need to be put in place to address this situation.

VII. CONCLUSIONS

85. ISPs' increasing reliance on monitoring and inspection techniques impinges upon the neutrality of the Internet and the confidentiality of communications. This raises serious issues relating to the protection of users' privacy and personal data.
86. While the Commission's Communication on the open internet and net neutrality in Europe briefly touches on these issues, the EDPS feels that more should be done in order to come to a satisfactory policy on the way forward. In this Opinion he has therefore contributed to the ongoing policy debate on net neutrality, particularly on aspects related to data protection and privacy.
87. The EDPS considers that there is a need for national authorities and BEREC to monitor the market situation. This monitoring should result in a clear picture describing whether the market is evolving towards massive, real-time inspection of communications and issues related to complying with the legal framework.
88. Monitoring of the market should not go without further analysis of the effects of new practices in relation to data protection and privacy on the Internet. This Opinion outlines some areas that would benefit from clarification. While EU agencies and bodies such as BEREC, the Article 29 Working Party and the EDPS may be in a good position to clarify the conditions of application of the framework, the EDPS considers that the Commission has a duty to coordinate and steer the debate. Therefore, he calls upon the Commission to take an initiative involving all those stakeholders in a platform or a working group, with this goal. Among the issues needing further analysis, the following points should be addressed:
- Determining the inspection practices that are legitimate to ensure the smooth flow of traffic and which can be carried out for security purposes;
 - Determining when monitoring requires individual's consent, notably the consent of all the users concerned, and the permissible technical parameters to ensure that the inspection technique does not entail processing of data that is not proportionate vis-à-vis its intended purpose.
 - In the cases above, guidance may be needed regarding the application of the necessary data protection safeguards (purpose limitation, security, etc.).
89. Depending on these findings, additional legislative measures may be necessary. In such a case, the Commission should put forward policy measures aiming at strengthening the legal framework and ensuring legal certainty. New measures should clarify the practical consequences of the net neutrality principle, as this has already been done in some Member States, and ensure that users can exercise a real choice, notably by forcing ISPs to offer non-monitored connections.

Done in Brussels, 7 October 2011

(signed)

Peter HUSTINX
European Data Protection Supervisor



Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"

Table of Content

A. GENERAL PART

1. Introduction	(§§ 1-12)
1.1. <i>A first and general assessment</i>	(§§ 1-6)
1.2. <i>Aim of the opinion</i>	(§§ 7-8)
1.3. <i>The building blocks of this opinion</i>	(§§ 9-12)
2. Context	(§§ 13-17)
3. Main perspectives	(§§ 18-42)
3.1. <i>Data protection fosters trust and must support other (public) interests</i>	(§§ 18-24)
3.2. <i>Consequences for the legal framework on data protection</i>	(§§ 25-42)

B. ELEMENTS OF A NEW FRAMEWORK

4. Comprehensive approach	(§§ 43-48)
5. Further harmonisation and simplification	(§§ 49-67)
5.1. <i>The need for harmonisation</i>	(§§ 49-51)
5.2. <i>Reducing the margin of manoeuvre in the implementation</i>	(§§ 52-53)
5.3. <i>Areas for further harmonisation</i>	(§§ 54-59)
5.4. <i>Simplification of the notification system</i>	(§§ 60-63)
5.5. <i>A Regulation, not a Directive</i>	(§§ 64-67)
6. Strengthening the rights of individuals	(§§ 68-98)
6.1. <i>The need for strengthening the rights</i>	(§§ 68-70)
6.2. <i>Increasing transparency</i>	(§§ 71-74)
6.3. <i>Support for an obligation to report security breaches</i>	(§§ 75-77)
6.4. <i>Reinforcing consent</i>	(§§ 78-82)
6.5. <i>Data portability and the right to be forgotten</i>	(§§ 83-91)
6.6. <i>Processing of personal data related to children</i>	(§§ 92-94)
6.7. <i>Collective redress mechanisms</i>	(§§ 95-98)
7. Strengthening the role of organisations/controllers	(§§ 99-117)
7.1. <i>General</i>	(§§ 99-100)
7.2. <i>Reinforcing data controllers' accountability</i>	(§§ 101-107)
7.3. <i>Privacy by design</i>	(§§ 108-115)
7.4. <i>Certification services</i>	(§§ 116-117)
8. Globalisation and applicable law	(§§ 118-127)
8.1. <i>A clear need for more consistent protection</i>	(§ 118)
8.2. <i>Investing in international rules</i>	(§§ 119-121)
8.3. <i>Clarifying applicable law criteria</i>	(§§ 122-125)
8.4. <i>Streamlining mechanisms for data flows</i>	(§§ 126-127)
9. The Area of police and justice	(§§ 128-136)
9.1. <i>The general framework</i>	(§§ 128-130)
9.2. <i>Additional specific rules for police and justice</i>	(§§ 131-133)
9.3. <i>Sector specific data protection regimes</i>	(§§ 134-136)
10. DPAs and the Cooperation between DPAs	(§§ 137-160)
10.1. <i>Reinforcing the role of DPAs</i>	(§§ 137-140)
10.2. <i>Strengthening the role of the Working Party</i>	(§§ 141-144)
10.3. <i>The advisory role of the Working Party</i>	(§§ 145-146)
10.4. <i>Coordinated enforcement by the Working Party</i>	(§§ 147-151)
10.5. <i>Cooperation between the EDPS and the Working Party</i>	(§§ 152-155)
10.6. <i>Cooperation between the EDPS and the DPAs in supervision on EU systems</i>	(§§ 156-160)

C. HOW TO IMPROVE APPLICATION OF PRESENT FRAMEWORK?

11. The short term	(§§ 161-166)
---------------------------	---------------------

D. CONCLUSIONS

Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data², and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION

A. GENERAL PART

1. Introduction

1.1. A first and general assessment

1. On 4 November 2010, the Commission adopted a Communication entitled "A comprehensive approach on personal data protection in the European Union" (the "Communication")³. The Communication was sent to the EDPS for consultation. The EDPS welcomes the fact that he was consulted by the Commission in accordance with Article 41 of Regulation (EC) No. 45/2001. Already before the adoption of the Communication the EDPS was given the possibility to give informal comments. Some of these comments have been taken into account in the final version of the document.
2. The Communication intends to lay down the Commission's approach for the review of the EU legal system for the protection of personal data in all areas of the Union's activities,

¹ OJ 1995, L 281/31.

² OJ 2001, L 8/1.

³ COM (2010) 609 final.

taking account, in particular, of the challenges resulting from globalisation and new technologies.⁴

3. The EDPS welcomes the Communication in general, as he is convinced that a review of the present legal framework for data protection in the EU is necessary, in order to ensure effective protection in a further developing information society. Already in his Opinion of 25 July 2007 on the Implementation of the Data Protection Directive⁵ he concluded that in the longer term, changes of Directive 95/46/EC seem unavoidable.
4. The Communication represents an important step towards such a legislative change which in turn would be the most important development in the area of EU data protection since the adoption of Directive 95/46/EC which is generally considered as the main cornerstone of data protection within the European Union (and wider within the European Economic Area).
5. The Communication gives the right framework for a well targeted review, also because it identifies - generally spoken - the main issues and challenges. The EDPS shares the view of the Commission that a strong system of data protection will still be needed in the future, based on the notion that existing general principles of data protection are still valid in a society which undergoes fundamental changes due to rapid technological developments and globalisation. This requires reviewing existing legislative arrangements.
6. The Communication rightly emphasises that the challenges are enormous. The EDPS fully shares this statement and underlines the consequence that the proposed solutions should be correspondingly ambitious and should enhance the effectiveness of the protection.

1.2. Aim of the opinion

7. This opinion assesses the proposed solutions in the Communication on the basis of these two criteria: ambition and effectiveness. Its perspective is positive in general. The EDPS supports the Communication, but is at the same time critical on aspects where in his view more ambition would lead to a more effective system.
8. The EDPS aims to contribute with this opinion to the further development of the legal framework on data protection. He looks forward to the Proposal of the Commission which is expected by mid 2011 and hopes that his suggestions will be taken into account in the wording of this proposal. He also notes that the Communication seems to exclude certain areas, such as data processing by EU institutions and bodies, from the general instrument. If the Commission would indeed decide to leave out certain areas at this stage – which the EDPS would regret - he urges the Commission to commit itself to realise a fully comprehensive architecture within a short and specified timeframe.

1.3. The building blocks of this opinion

9. This opinion does not stand alone. It is based on earlier positions taken by the EDPS and by the European data protection authorities on various occasions. In particular, it must be underlined that in the already mentioned EDPS Opinion of 25 July 2007 some main

⁴ See p. 5 of the Communication, first paragraph.

⁵ EDPS Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 1.

elements for future change were identified and developed.⁶ It is also based on discussions with other stakeholders in the areas of privacy and data protection. Their contributions offered a very useful background for both the Communication and this opinion. In this regard, it can be concluded that there exists a level of synergy on how to improve effectiveness of data protection.

10. Another important building block of this Opinion is the document called 'The Future of Privacy', the Joint contribution of the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation launched by the Commission in 2009 (the "WP document on the Future of Privacy").⁷
11. More recently, at a Press Conference on 15 November 2010, the EDPS gave his first reactions on the present Communication. This opinion elaborates the more general views brought forward during this Press Conference.⁸
12. Finally, this Opinion profits from a number of earlier EDPS Opinions, as well as from documents of the Article 29 Data Protection Working Party. References to those opinions and documents can be found in various places of this opinion, where relevant.

2. Context

13. The review of data protection rules occurs at a crucial historical moment. The Communication describes the context extensively and in a convincing way. Based on this description the EDPS identifies the four main drivers determining the environment in which the review process takes place.
14. The first driver is technological development. Today's technology is not the same as when Directive 95/46 was conceived and adopted. Technological phenomena like cloud computing, behavioural advertising, social networks, road toll collecting and geo-location devices profoundly changed the way in which data are processed and pose enormous challenges for data protection. A review of European data protection rules will have to address these challenges effectively.
15. The second driver is globalisation. The progressive abolition of trade barriers has given businesses an increasing worldwide dimension. Cross border data processing and international transfers have tremendously increased over the past years. Furthermore, data processing has become ubiquitous due to Information and Communication Technologies: internet and cloud computing allowed delocalised processing of large quantities of data on a worldwide scale. The last decade also witnessed an increase in international police and judicial activities to fight terrorism and other forms of international organised crime, supported by an enormous exchange of information for law enforcement purposes. All this calls for a serious consideration of how personal data protection can be ensured

⁶ In particular (see point 77 of the opinion): no need to change existing principles, but a clear need for other administrative arrangements; the wide scope of data protection law applicable to all use of personal data should not change; data protection law should allow a balanced approach in concrete cases and should also allow data protection authorities to set priorities; the system should fully apply to the use of personal data for law enforcement purposes, although appropriate additional measures may be necessary to deal with special problems in this area.

⁷ Document WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Its main message is that a legislative change is a good opportunity to clarify some key rules and principles (e.g. consent, transparency), introduce some new principles (e.g. privacy by design, accountability), strengthen the effectiveness by modernising the arrangements (e.g. by limiting existing notification requirements) and include all into one comprehensive legal framework (incl. police and judicial cooperation).

⁸ The Speaking Points for the Press Conference are available on the EDPS website, at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf.

effectively in the globalised world without substantially hampering international processing activities.

16. The third driver is the Lisbon Treaty. The entry into force of the Lisbon Treaty marks a new era for data protection. Article 16 TFEU not only contains an individual right of the data subject, but also provides a direct legal basis for a strong EU-wide data protection law. Furthermore, the abolition of the pillar structure obliges the European Parliament and Council to provide for data protection in all areas of EU law. In other words, it allows for a comprehensive legal framework for data protection applicable to the private sector, the public sector in the Member States and the EU institutions and bodies. The Stockholm Programme⁹ consistently states in this regard that the Union must secure a comprehensive strategy to protect data within the EU and in its relations with other countries.
17. The fourth driver is represented by parallel developments taking place in the context of international organisations. There are various ongoing debates focussing on the modernisation of the current legal instruments for data protection. It is important to mention in this respect the current reflections undertaken in relation to the future revision of Convention 108 of the Council of Europe¹⁰ and of the OECD Privacy Guidelines.¹¹ Another important development regards the adoption of international standards on the protection of personal data and privacy, which might possibly lead to the adoption of a binding global instrument on data protection. All these initiatives deserve full support. Their common goal should be ensuring effective and consistent protection in a technologically driven and globalised environment.

3. Main perspectives

3.1. Data protection fosters trust and must support other (public) interests

18. A strong framework for data protection is the necessary consequence of the importance given to data protection under the Lisbon Treaty, in particular in Article 8 of the Charter of the Fundamental Rights of the Union and Article 16 TFEU, as well as the strong link with Article 7 of the Charter.¹²
19. However, a strong framework for data protection also serves wider public and private interests in an information society with ubiquitous data processing. Data protection fosters trust, and trust is an essential component of the well functioning of our society. It is essential that arrangements for data protection are construed in a way that they - as much as possible - actively support rather than hamper other legitimate rights and interests.
20. Important examples of other legitimate interests are a strong European economy, the security of individuals, as well as the accountability of governments.
21. Economic development in the EU goes hand in hand with the introduction and the marketing of new technologies and services. In the information society the emergence and successful deployment of information and communications technologies and services

⁹ The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJ C115, 04/05/2010, p. 1-38, at p. 10.

¹⁰ Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data, ETS No 108, 28.1.1981.

¹¹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, published on www.oecd.org.

¹² This importance of data protection and the link with privacy in the Charter were underlined by the Court of Justice in its Judgment of 9 November 2010, Joint Cases C-92/09 and C-93/09, *Schecke*, not yet published in ECR.

depends on trust. If people do not trust ICT, these technologies are likely to fail.¹³ And people will only trust ICT if their data are efficiently protected. Therefore, data protection should be an integral part of technologies and services. A strong framework for data protection fosters the European economy, provided that this framework is not only strong but also tailored in the right way. Further harmonisation within the EU and minimisation of administrative burdens are in this perspective essential (see Chapter 5 of the opinion).

22. Much has been said in recent years about the need for balancing privacy and security, especially in relation to instruments for data processing and exchange in the area of police and judicial cooperation.¹⁴ Data protection was quite often wrongly characterised as an obstacle to fully protecting the physical security of individuals¹⁵, or at least as an unavoidable condition to be respected by law enforcement authorities. However, this is not the whole story. A strong framework of data protection can sharpen and strengthen security. On the basis of principles of data protection - when applied well - controllers are obliged to ensure that information is accurate and up to date, and that superfluous personal data that are not necessary for law enforcement are eliminated from the systems. One can equally point to obligations to implement technological and organisational measures to ensure the security of systems such as protecting systems against unauthorised disclosure or access, as developed in the field of data protection.
23. Respecting principles of data protection may further ensure that law enforcement authorities operate under the rule of law which triggers trust in their behaviour and therefore fosters in a wider sense trust in our societies. The case law developed under Article 8 of the European Convention of Human Rights ensures that police and judicial authorities can process all data relevant for their work, but not in an unlimited manner. Data protection requires checks and balances (see on police and justice Chapter 9 of the opinion).
24. In democratic societies governments are accountable for all their activities, including for their use of personal data for the different public interests they serve. This varies from publication of data on the internet for reasons of transparency, to the use of data as a support of policies in areas like public health, transport or taxation, or the surveillance of individuals for law enforcement purposes. A strong data protection framework allows governments to respect their responsibilities and to be accountable, as part of good governance.

3.2. Consequences for the legal framework on data protection

3.2.1. Further harmonisation is needed

25. The Communication rightly identified that one of the essential shortcomings of the current framework is that it leaves too much discretion to the Member States in the implementation of the European provisions into national law. Lack of harmonisation has a number of negative consequences in an information society where the physical borders between the Member States are less and less relevant (see Chapter 5 of the opinion).

3.2.2. General principles of data protection still remain valid

¹³ See EDPS Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy, OJ C 280, 16.10.2010, p. 1, para 113.

¹⁴ See e.g. EDPS Opinion of 10 July 2009 on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen, OJ C 276, 17.09.2009, p. 8

¹⁵ Security is a wider notion than physical security, but as an illustration of the arguments at stake it is here used in its more limited sense.

26. A first and more formal reason why the general principles of data protection should and could not be changed is of a legal nature. These principles are laid down in Council of Europe Convention 108 which is binding on all the Member States. This Convention is the basis of data protection in the EU. Moreover, some of the main principles are explicitly mentioned in Article 8 of the Charter of the Fundamental rights of the Union. Changing of these principles would thus require changing the Treaties.
27. However, this is not the full story. There are also substantial reasons not to change the general principles. The EDPS strongly believes that an information society can and should not function without an adequate protection of privacy and personal data of individuals. When more information is being processed, also better protection is needed. An information society where abundant amounts of information about everyone are being processed needs to be built on the concept of control by the individual, in order to allow him or her to act as an individual and to use his freedoms in a democratic society such as the freedoms of expression and speech.
28. Furthermore, it is difficult to imagine control of the individual without obligations on controllers to limit processing in accordance with principles of necessity, proportionality and purpose limitation. It is equally difficult to imagine control by the individual in the absence of recognised data subjects' rights, such as the rights of access, rectification, erasure or blocking of data.

3.2.3. *Fundamental rights perspective*

29. The EDPS underlines that data protection is recognised as a fundamental right. This does not mean that data protection should always *prevail* over other important rights and interests in a democratic society, but it does have consequences for the nature and scope of the protection that must be given under an EU legal framework, so as to ensure that data protection requirements are always *adequately* taken into account.
30. These main consequences can be defined as follows:
- Protection must be effective. A legal framework must provide for instruments that make it feasible for individuals to exercise their rights in practice.
 - The framework must be stable over a long period.
 - Protection must be given under all circumstances and not depend on the political preferences in a certain timeframe.
 - Limitations to the exercise of the right may be needed, but they must be exceptional, duly justified and never affect the essential elements of the right itself.¹⁶
- The EDPS recommends that the Commission take these consequences into account when proposing legislative solutions.

3.2.4. *New legislative arrangements are needed*

31. The Communication rightly concentrates on the need for strengthening the legislative arrangements for data protection. In this context, it makes sense to recall that in the WP document on the Future of Privacy¹⁷ the Data Protection Authorities emphasised the need

¹⁶ See also the EDPS Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, para 17, which builds on the case law of the European Court of Human Rights and the Court of Justice.

¹⁷ See footnote 7.

for stronger roles for the different actors in the field of data protection, notably the data subjects, the data controllers and the supervisory authorities themselves.

32. There seems to be a wide consensus amongst stakeholders that stronger legislative arrangements - taking into account technological developments and globalisation - are the key towards ambitious and effective data protection also in the future. As already indicated in point 7, these are the criteria for the assessment of the EDPS of any proposed solutions.

3.2.5. *Comprehensiveness as a conditio sine qua non*

33. As recalled in the Communication, Directive 95/46 applies to all personal data processing activities in Member States in both the public and the private sectors, with exception of activities which fall outside the scope of former Community law¹⁸. Whilst this exception was needed under the former Treaty, this is no longer the case after the entry into force of the Lisbon Treaty. Moreover, the exception is contrary to - the text and in any event the spirit of - Article 16 TFEU.

34. According to the EDPS, a comprehensive legal instrument for data protection including police and judicial cooperation in criminal matters must be seen as one of the main improvements a new legal framework can bring. It is a *conditio sine qua non* for effective data protection in future.

35. The EDPS highlights the following arguments in support of this statement:

- The distinction between activities of the private sector and of the law enforcement sector is blurring. Private sector entities may process data which are ultimately used for law enforcement purposes (example: PNR data¹⁹), whilst in other cases, they are required to keep data for law enforcement purposes (example: Data Retention Directive²⁰).
- There is no fundamental difference between police and judicial authorities and other authorities delivering law enforcement (taxation, customs, anti-fraud, immigration) subject to Directive 95/46.
- As accurately described in the Communication, the data protection legal instrument currently applicable to police and judicial authorities (Framework Decision 2008/977²¹) is inadequate.
- Most Member States have implemented Directive 95/46 and Convention 108 in their national legislations, making them applicable also to their police and judicial authorities.

36. Including police and justice in the general legal instrument would not only offer more guarantees to citizens but also make the task of police authorities easier. Having to apply various sets of rules is cumbersome, needlessly time-consuming and stands in the way of international cooperation (see further Chapter 9 of the opinion). This also argues for

¹⁸ This opinion will mainly focus on the former 3rd pillar (police and judicial cooperation in criminal matters), since the former 2nd pillar is not only a more complicated area of EU law (as also recognised by Article 16 TFEU and Article 39 EU), but also to a lesser extent relevant for data processing.

¹⁹ See e.g. Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM (2010) 492 final.

²⁰ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105/ 54).

²¹ Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

including the processing activities by national security services, in so far as this is possible under the current state of EU law.

3.2.6. Technological neutrality

37. The period since the adoption of Directive 95/46 in 1995 can be characterised as technologically turbulent. New technological developments and appliances are introduced on a frequent basis. In many cases this has led to fundamental changes in the way personal data of individuals are being processed. The information society can no longer be considered as a parallel environment where individuals can participate on a voluntary basis, but has become an integrated part of our day to day lives. Just as an example, the concept of an Internet of things²² establishes links between physical objects and on line information related to them.
38. Technology will further develop. This has its consequences for the new legal framework. It must be effective for a greater number of years, and at the same time not hamper further technological developments. This requires that the legal arrangements are technologically neutral. However, the framework must also bring more legal certainty for companies and for individuals. They must understand what is expected from them and be able to exercise their rights. This requires that the legal arrangements are precise.
39. According to the EDPS, a general legal instrument for data protection must be formulated in a technologically neutral way, as far as possible. This implies that the rights and obligations of the various actors are to be formulated in a general and neutral way so as to remain, in principle, valid and enforceable irrespective of the technology chosen for processing personal data. There is no other choice, given the fast pace of technology advancements nowadays. The EDPS suggests introducing new 'technologically neutral' rights on top of the existing principles of data protection which could have a specific importance in the rapidly changing electronic environment (see mainly Chapters 6 and 7).

3.2.7. Long term: Legal certainty for a longer period

40. Directive 95/46 has been the central piece of data protection in the EU for the last 15 years. It was implemented in the laws of the Member States and applied by the different actors. Over the years the application has profited from practical experiences and from further guidance given by the Commission, the Data Protection Authorities (on the national level and in the framework of the Article 29 Working Party) and national and European Courts.
41. It is good to emphasise that these developments need time and that - especially since we deal with a general framework giving effect to a fundamental right - this time is needed to create legal certainty and stability. A new general legal instrument needs to be drafted with the ambition that it will be able to create legal certainty and stability for a longer period, keeping in mind that it is very difficult to predict how technology and globalisation will further develop. In any event, the EDPS fully supports the aim to create legal certainty for a longer period, comparable to the perspective of Directive 95/46. In short, where technology develops at a fast pace, the law must be stable.

3.2.8. Short term: Make better use of existing instruments

²² As defined in 'Internet of things - An action plan for Europe', COM (2009) 278 Final.

42. In the short term, it is essential to ensure the effectiveness of existing legislative arrangements, in the first place by concentrating on enforcement, at national and at EU level (see Chapter 11 of this opinion).

B. ELEMENTS OF A NEW FRAMEWORK

4. Comprehensive approach

43. The EDPS fully supports the comprehensive approach on data protection which is not only the title but also the point of departure of the Communication and necessarily includes the extension of the general rules on data protection to police and judicial cooperation in criminal matters.²³

44. However, he also notes that the Commission does not intend to include all data processing activities in this general legal instrument. In particular, data processing by EU institutions, bodies, offices and agencies will not be included. The Commission only states that it 'will assess the need to adapt other legal instruments to the new general data protection framework'.

45. The EDPS has a clear preference for including processing on the EU level in the general legal framework. He reminds that this was the original intention of the former Art 286 EC which mentioned data protection for the first time on the level of the Treaty. Article 286 EC simply stated that legal instruments on the processing of personal data would apply to the institutions as well. More importantly, one legal text avoids the risk of discrepancies between provisions and would be most suitable for data exchange between the EU level and the public and private entities in the Member States. It would also avoid the risk that, after modifying Directive 95/46, there is no political interest any more in amending Regulation 45/2001 or to give this modification sufficient priority to avoid discrepancies in dates of entry into force.

46. The EDPS urges the Commission - in case it would conclude that the inclusion of processing at the EU level in the general legal instrument would not be feasible - to commit itself to propose an adaptation of Regulation 45/2001 (not to 'assess the need') within the shortest possible timeframe and preferably by the end of 2011.

47. It is equally important that the Commission ensures that other areas do not stay behind, in particular:

- Data protection in the Common Foreign and Security Policy, on the basis of Article 39 TEU.²⁴
- Sector specific data protection regimes for EU bodies such as Europol, Eurojust and for large scale information systems, in so far as they need to be adapted to the new legal instrument.
- The ePrivacy Directive 2002/58, in so far as it needs to be adapted to the new legal instrument.

48. Finally, a general legal instrument for data protection may and probably must be complemented by additional sectoral and specific regulations, for instance for police and

²³ See p. 14 of the Communication and Section 3.2.5 of this opinion.

²⁴ See also EDPS Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges, point 31.

judicial cooperation, but also in other areas.²⁵ Where needed and in conformity with the principle of subsidiarity, those additional regulations should be adopted at EU level. Member States may draw up additional rules, in specific areas where this is justified (see 5.2).

5: Further harmonisation and simplification

5.1. The need for harmonisation

49. Harmonisation is of paramount importance for EU data protection law. The Communication correctly stressed that data protection has a strong internal market dimension, as it must ensure the free flow of personal data between Member States within the internal market. However, the level of harmonisation under the present Directive has been judged as less than satisfactory. The Communication recognises that this is one of the main recurrent concerns of stakeholders. In particular, stakeholders stress the need to enhance legal certainty, reduce the administrative burden and ensure a level playing field for economic operators. As the Commission rightly notes, this is particularly the case for data controllers established in several Member States and obliged to comply with the (possibly diverging) requirements of national data protection laws.²⁶

50. Harmonisation is not only important for the internal market but also with a view to ensuring adequate data protection. Article 16 of the TFEU provides that “everyone” has the right to the protection of personal data concerning them. In order for this right to be effectively respected, an equivalent level of protection must be guaranteed throughout the EU. The WP document on the Future of Privacy highlighted that several provisions relating to data subjects' positions have not been implemented or interpreted uniformly in all Member States²⁷. In a globalised and interconnected world, these divergences could undermine or limit the protection of individuals.

51. The EDPS believes that further and better harmonisation is one of the principal objectives of the review process. The EDPS welcomes the Commission’s commitment to examine the means to achieve further harmonisation of data protection at EU level. However, he notes with some surprise that the Communication does not put forward at this stage any concrete options. He therefore indicates himself a few areas where greater convergence is most urgent (see 5.3). Further harmonisation in these areas should not only be achieved by reducing the margin of manoeuvre for national law, but also preventing incorrect implementation by Member States (see also Chapter 11) and ensuring more consistent and coordinated enforcement (see also Chapter 10).

5.2. Reducing the margin of manoeuvre in the implementation of the Directive

52. The Directive contains a number of provisions that are broadly formulated and that therefore leave significant room for diverging implementation. Recital 9 of the Directive explicitly confirms that Member States are given a certain margin of manoeuvre and that, within this margin, disparities could arise in the implementation of the Directive. Several provisions have been implemented differently by Member States, including some crucial provisions²⁸. This situation is not satisfactory and greater convergence should be sought.

²⁵ See also WP document on the Future of Privacy (footnote 7), points 18-21.

²⁶ Communication, p. 10.

²⁷ See WP document on the Future of Privacy (footnote 7), point 70. The document refers in particular to liability provisions and the possibility to claim immaterial damages.

²⁸ Some divergent approaches also exist with regard to manual data.

53. This does not mean that diversity should be excluded outright. In certain areas flexibility might be needed in order to preserve justified specificities, important public interests or the institutional autonomy of the Member States. According to the EDPS, room for divergence between the Member States should be limited in particular to the following specific situations:

- Freedom of expression: under the present framework (Article 9), Member States may provide for exemptions and derogations in relation to the processing of data carried out for journalistic purposes or for the purpose of artistic or literary expression. This flexibility appears well placed, subject of course to limits in the Charter and ECHR, given the different traditions and cultural differences that may exist in this field across Member States. However, this would not stand in the way of a possible update of the current Article 9 in the light of developments on the Internet.
- Specific public interests: under the present framework (Article 13), Member States may adopt legislative measures to restrict the scope of the obligations and rights when such a restriction constitutes a necessary measure to safeguard important public interest, such as national security, defence, public security, etc. This competence of Member States remains justified. However, where possible, the interpretation of the exceptions should be further harmonised (see Section 9.1). In addition, the current scope for exception to Article 6(1) appears unduly wide.
- Legal remedies, sanctions and administrative procedures: a European framework should determine the main conditions, but under the current state of EU law the determination of sanctions, legal remedies, procedural rules and the modalities of inspections as applicable at national level must be left to Member States.

5.3. Areas for further harmonisation

54. Definitions (Article 2 of Directive 95/46). Definitions are the cornerstone of the legal system and should be uniformly interpreted in all Member States, with no margin of implementation. Divergences have arisen under the present framework, like for example as to the notion of controller²⁹. The EDPS suggests adding further items to the current list in Article 2 in order to provide for more legal certainty, such as anonymous data, pseudonymous data, judicial data, data transfer and data protection officer.

55. Lawfulness of processing (Article 5). The new legal instrument should be as precise as possible with regard to the core elements determining the lawfulness of data processing. Article 5 of the Directive (as well as its Recital 9), mandating Member States to determine more precisely the conditions under which the processing is lawful, may thus be no longer needed in a future framework.

56. Grounds for data processing (Article 7 and 8). The definition of the conditions for data processing is an essential element of any data protection legislation. Member States should not be allowed to introduce additional or modified grounds for processing or to exclude any. The possibility of derogations should be excluded or limited (particularly with regard to sensitive data³⁰). In a new legal instrument the grounds for data processing should be clearly formulated, thereby reducing the margin of appreciation in the implementation or enforcement. In particular, the notion of consent may need to be further specified (see Section 6.5). Moreover, the ground based on the legitimate interest of the data controller (Article 7, letter (f)), gives way to widely diverging interpretations, due to

²⁹ See WP 29 Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

³⁰ Article 8(4) and (5) currently authorize under certain conditions Member States to provide for further derogations with regard to sensitive data.

its flexible nature. Further specification is needed. Another provision that possibly must be specified is Article 8(2)(b), allowing the processing of sensitive data necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law³¹.

57. Data subject rights (Articles 10-15). This is one of the areas in which not all elements of the Directive have been consistently implemented and interpreted by Member States. Data subjects' rights are a central element for an effective data protection. As a consequence, the room for manoeuvre should be substantially reduced. The EDPS recommends that the information provided to data subjects by the controller should be uniform across the EU.
58. International transfers (Articles 25-26). This is an area which has given rise to widespread criticism because of the lack of a uniform practice throughout the EU. Stakeholders criticised that the Commission's decisions on adequacy are interpreted and implemented very differently by the Member States. Binding Corporate Rules (BCRs) are a further element where the EDPS recommends further harmonisation (see Chapter 9).
59. National Data Protection Authorities (Article 28). National DPAs are subject to widely diverging rules in the 27 Member States, particularly with regard to their status, resources and powers. Article 28 has partly contributed to this divergence because of its lack of precision³² and should be further specified, in conformity with the Judgment of the European Court of Justice in Case C-518/07³³ (see further Chapter 10).

5.4. Simplification of the notification system

60. Notification requirements (Article 18-21 of Directive 95/46) are another field where Member States have so far been granted significant freedom. The Communication rightly recognises that a harmonised system would reduce costs as well as administrative burden for data controllers³⁴.
61. This is an area where simplification should be the main objective. The review of the data protection framework is a unique opportunity to further simplify and/or reduce the scope of the current notification requirements. The Communication recognises that there is a general consensus amongst stakeholders that the current system of notifications is rather cumbersome and does not provide, in itself, added value for the protection of individuals' personal data.³⁵ The EDPS thus welcomes the Commission's commitment to explore different possibilities for the simplification of the current notification system.
62. In his view, the point of departure of this simplification would be a shift from a system where notification is the rule, save as otherwise provided (i.e., "exemption system"), to a more targeted system. The exemption system proved to be inefficient, as it was implemented in an inconsistent way across Member States.³⁶ The EDPS suggests considering the following alternatives:

³¹ See, in this regard, the Commission's First Report on the implementation of the Data Protection Directive, cited above, p. 14.

³² WP document on the Future of Privacy, para 87.

³³ Case C-518/07, *Commission v. Germany*, not yet published in ECR.

³⁴ Communication, p. 10.

³⁵ Communication, p. 10.

³⁶ Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplifications and the role of the data protection officers in the European Union, WP 106, 2005, p. 7.

- Limit the obligation to notify to specific kinds of processing operations entailing specific risks (these notifications could trigger further steps such as prior checking of the processing).
- A simple registration obligation requiring data controllers to register (as opposed to extensive registration of all data processing operations).

In addition, a standard pan-European notification form could be introduced so as to ensure harmonised approaches with regard to the information requested.

63. The review of the current notification system should be without prejudice to improving prior-checking obligations for certain processing obligations likely to present specific risks (such as large scale information systems). The EDPS would favour the inclusion in the new legal instrument of a non-exhaustive list of cases where such prior-checking is required. Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by EU institutions and bodies provides a useful model for this purpose³⁷.

5.5. A Regulation, not a Directive

64. Finally, the EDPS believes that the review process is also an opportunity to reconsider the type of legal instrument for data protection. A Regulation, a single instrument which is directly applicable in the Member States, is the most effective means to protect the fundamental right to data protection and to create a real internal market where personal data can move freely and where the level of protection is equal independently of the country or the sector where the data are processed.

65. A Regulation would reduce room for contradictory interpretations and for unjustified differences in the implementation and the application of the law. It would also reduce the importance of determining the law applicable to processing operations within the EU, which is one of the most controversial aspects of the present system (see Chapter 9).

66. In the area of data protection a Regulation is all the more justified, since

- Article 16 TFEU has upgraded the right to the protection of personal data to the Treaty level and envisages – or even mandates – a uniform level of protection of individual throughout the EU.
- Data processing takes place in an electronic environment where internal borders between the Member States have become less relevant.

67. The choice for a Regulation as a general instrument allows, where necessary, provisions directly addressed to Member States where flexibility is needed. It also does not influence the competence of Member States to adopt additional rules for data protection, where needed, in conformity with EU law.

6. Strengthening the rights of individuals

6.1. The need for strengthening the rights

68. The EDPS fully supports the Communication where it proposes strengthening individuals' rights, since existing legal instruments do not fully deliver the effective protection that is needed in an increasingly complex digitalized world.

³⁷ See Article 27 of the Regulation, OJ 2001, L 8/1.

69. On the one hand, the development of a digitalized world entails a sharp growth in the collection, use and further transfer of personal data in an extremely complex and non transparent way. Individuals are often not aware or do not understand how this happens, who collects their data, nor how to exercise control. An illustration of this phenomenon is the monitoring by ad network providers of individuals' web browsing activities, using cookies or similar devices, for the purposes of targeted advertising. When users visit web sites, they do not expect that an out of sight third party logs such visits and creates users' records, based on information revealing their life style, or what they like or dislike.

70. On the other hand, the development stimulates individuals pro-actively sharing their personal information, for example on social networks. Increasingly young people are part of a social network and interact with their peers. It is doubtful whether (young) people, are aware of the breadth of their disclosure and of the long term effects of their actions.

6.2. Increasing transparency

71. Transparency is of paramount importance in any data protection regime, not only because of its inherent value but also because it enables other data protection principles to be exercised. Only if individuals know about the data processing, they will be able to exercise their rights.

72. Several provisions in Directive 95/46 deal with transparency. Article 10 and 11 contain an obligation to give information to individuals about the collection of their personal data. Moreover, Article 12 recognizes the right to receive a copy of one's own personal data in an intelligible form (right of access). Article 15 recognises the right to have access to the logic on which automated decisions producing legal effects are made. Last but not least, Article 6.1(a) requiring the processing to be fair also entails a transparency requirement. Personal data cannot be processed for any hidden or secret reasons.

73. The Communication suggests adding a general principle of transparency. In reaction to this suggestion, the EDPS underlines that the notion of transparency is already an integral part of the present legal framework on data protection, albeit in an implicit way. This can be deduced from the various provisions dealing with transparency, as mentioned in the preceding paragraph. According to the EDPS, it could have added value to include an *explicit* principle of transparency, either or not linked to the existing provision of fair processing. This would increase legal certainty and also confirm that a controller should under all circumstances process personal data in a transparent way, not only on request or when a specific legal provision requires him to do so.

74. However, it is perhaps more important to reinforce the existing provisions dealing with transparency, such as the existing Articles 10 and 11 of Directive 95/46. Those provisions specify the information elements that must be provided, but are not precise on the modalities. More concretely, the EDPS suggests strengthening the existing provisions by:

- A requirement for a controller to provide information on data processing in a manner which is easily accessible and easy to understand, and in clear and plain language³⁸. The information should be clear, conspicuous and prominent. The provision could also encompass the obligation to ensure easy understanding of the information. This obligation would render illegal privacy policies which are opaque or difficult to understand.

³⁸ See Communication, p. 6.

- A requirement to render the information easily and directly to data subjects. The information should also be permanently accessible, and not after a very short time disappear from an electronic medium. This would help users to store and reproduce information in the future, enabling further access.

6.3. Support for an obligation to report security breaches

75. The EDPS supports the introduction of a provision on personal data breach notification in the general instrument, which extends the obligation which was included in the revised ePrivacy Directive for certain providers to all data controllers, as proposed in the Communication. Under the revised ePrivacy Directive the obligation only applies to providers of electronic communication services (providers of telephony (including VoIP) service and Internet access). Other data controllers are not covered by the obligation. The reasons that justify the obligation fully apply to data controllers other than providers of electronic communication services.

76. Security breach notification serves different purposes and aims. The most obvious one, highlighted by the Communication, is to serve as an information tool to make individuals aware of the risks they face when their personal data are compromised. This may help them to take the necessary measures to mitigate such risks. For example, when alerted of breaches affecting their financial information, individuals will be able, among other things, to change passwords or cancel their accounts. In addition, security breach notification contributes to the effective application of other principles and obligations in the Directive. For example, security breach notification requirements incentivize data controllers to implement stronger security measures to prevent breaches. Security breach is also a tool to strengthen the responsibility of data controllers and, more in particular to enhance accountability (see Chapter 7). Finally, it serves as a tool for the enforcement by DPAs. The notification of a breach to DPAs may lead to an investigation of the overall practices of a data controller.

77. The specific rules on security breach in the amended ePrivacy Directive were broadly discussed during the parliamentary phase of the legislative framework that preceded the adoption of the ePrivacy Directive. In this debate, the opinions of the Article 29 Working Party and EDPS were taken into consideration together with the views of other stakeholders. The rules reflect the views of different stakeholders. They represent a balance of interests: while the criteria triggering the obligation to notify are, in principle, adequate to protect individuals, they do so without imposing overly cumbersome, not useful requirements.

6.4. Reinforcing consent

78. Article 7 of the Data Protection Directive lists six legal bases for processing personal data. Consent of the individual is one of them. A data controller is allowed to process personal data to the extent in which individuals have given informed consent to have their data collected and further processed.

79. In practice, often users have limited control in relation to their data, particularly in technological environments. One of the methods that is sometimes used is implied consent, which is consent that has been inferred. It can be inferred from an action of the individual (e.g. the action consisting in using a web site is deemed as consenting to log user's data for marketing purposes). It can also be inferred from silence or inaction (not un-clicking a ticked box is deemed to be consent).

80. According to the Directive, for consent to be valid it must be informed, freely given and specific. It must be an informed indication of the individuals' wishes by which he signifies his agreement to personal data relating to him being processed. The way in which consent is given must be unambiguous.
81. Consent that has been inferred by an action and more particularly by silence or inaction is often not an unambiguous consent. However, it is not always clear what constitutes true, unambiguous consent. Some data controllers exploit this uncertainty by relying on methods not suitable to deliver true, unambiguous consent.
82. In light of the above, the EDPS supports the Commission on the need to clarify the limits of consent and to make sure that only consent that is construed in a solid way is taken as such. In this context, the EDPS suggests as follows³⁹:
- It could be considered to broaden the situations where express consent is required, currently limited to sensitive data.
 - Adopt additional rules for consent in the on-line environment.
 - Adopt additional rules for consent to process data for secondary purposes (i.e., the processing is secondary to the main processing or not an obvious one).
 - In an additional legislative instrument, either or not adopted by the Commission under Article 290 TFEU, determine the type of consent needed, for example, to specify the level of consent on the processing of data from RFID tags on consumer products or on other specific techniques.

6.5. Data portability and the right to be forgotten

83. Data portability and the right to be forgotten are two connected concepts put forward by the Communication to strengthen data subjects' rights. They are complementary to the principles already mentioned in the Directive, providing for a right for the data subject to object to the further processing of his/her personal data, and an obligation for the data controller to delete information as soon as it is no longer necessary for the purpose of the processing.
84. These two new notions have mostly added value in an information society context, where more and more data are automatically stored and kept for indefinite periods of time. Practice shows that, even if data are uploaded by the data subject himself, the degree of control he effectively has on his personal data is in practice very limited. This is all the more true in view of the gigantic memory the Internet represents today. Besides, from an economic perspective, it is more costly for a data controller to delete data than to keep them stored. The exercise of the rights of the individual therefore goes against the natural economic trend.
85. Both data portability and the right to be forgotten could contribute to shift the balance in favour of the data subject. The objective of data portability would be to give more control to the individual on his information, while the right to be forgotten would ensure that the information automatically disappears after a certain period of time, even if the data subject does not take action or is not even aware the data was ever stored.
86. More specifically, data portability is understood as the users' ability to change preference about the processing of their data, in connection in particular with new technology

³⁹ The WP 29 is currently working on an opinion on 'consent'. This opinion might lead to additional suggestions.

services. Increasingly, this applies to services that entail the storage of information, including personal data, such as mobile telephony and, services that store pictures, emails, and other information, sometimes using cloud computing services.

87. Individuals must easily and freely be able to change the provider and transfer their personal data to another service provider. The EDPS considers that existing rights set forth in Directive 95/46 could be reinforced by including a portability right in particular in the context of information society services, to assist individuals in ensuring that providers and other relevant controllers give them access to their personal information while at the same time ensuring that the old providers or other controllers delete that information even if they would like to keep it for their own legitimate purposes.
88. A newly codified "right to be forgotten" would ensure the deletion of personal data or the prohibition to further use them, without a necessary action of the data subject, but at the condition that this data has been already stored for a certain amount of time. The data would in other words be attributed some sort of expiration date. This principle is already affirmed in national court cases or applied in specific sectors, for instance for police files, criminal records or disciplinary files: under some national laws, information about individuals is automatically deleted or not to be further used or disseminated, especially after a fixed period of time, without need for a prior analysis on a case by case basis.
89. In this sense, a new "right to be forgotten" should be connected to data portability. The added value it would bring is that it would not require efforts or insistence from the data subject to have his data deleted, as this should be done in an objective and automated way. Only in very specific circumstances, where a specific need to keep data longer could be established, could a data controller be entitled to keep the data. That "right to be forgotten" would thus reverse the burden of proof from the individual to the data controller and constitute a "privacy by default" setting for the processing of personal data.
90. The EDPS considers that the right to be forgotten could prove especially useful in the context of information society services. An obligation to delete or not further disseminate information after a fixed period of time makes sense especially in the media or the internet, and notably in social networks. It would also be useful as far as terminal equipments are concerned: data stored on mobile devices or computers would be automatically deleted or blocked after a fixed period of time, when they are no more in the possession of the individual. In that sense the right to be forgotten can be translated in a "privacy by design" obligation.
91. In sum, the EDPS is of the opinion that data portability and the right to be forgotten are useful concepts. It could be worthwhile to include them in the legal instrument, but probably limited to the electronic environment.

6.6. Processing of personal data related to children

92. Under Directive 95/46 there are no particular rules regarding the processing of children's personal data. This does not recognise the need for a specific protection of children in specific circumstances, because of their vulnerability, and because it causes legal uncertainty, particularly in the following areas:
 - the collection of children's data and the way they must be informed about the collection;
 - the way children's consent is obtained. Because there are no specific rules on how to obtain children's consent and on the age under which children should be

considered as such, these subject are dealt with under national law, which differs from Member State to Member State⁴⁰;

- the way and conditions under which children or their legal representatives can exercise their rights under the Directive.

93. The EDPS considers that children's particular interests would be better protected if the new legal instrument contained additional provisions, specifically addressed to the collection and further processing of children's data. Such specific provisions would also provide legal certainty in this specific area and they would be to the benefit of data controllers who are currently exposed to different legal requirements.

94. The EDPS suggests including the following provisions in the legal instrument:

- A requirement for information to be adapted to children insofar as this would make it easier for children to understand what it means when data from them are collected.
- Other information requirements adapted to children, on the manner in which the information must be provided and possibly also on the content.
- A specific provision protecting children against behavioural advertising.
- The purpose limitation principle should be reinforced as far as children's data are concerned.
- Some categories of data should never be collected from children.
- An age threshold. Below such threshold, generally speaking information from children should be collected only with explicit and verifiable parental consent.
- If parental consent is necessary, it would be necessary to establish rules on how to authenticate the age of the child, in other words, how to know that the child is a minor and how to verify parental consent. This is an area where the EU can draw inspiration from other countries such as the United States⁴¹.

6.7. *Collective redress mechanisms*

95. Strengthening the substance of individuals' rights would be pointless, in the absence of effective procedural mechanisms to enforce such rights. In this context, the EDPS recommends the introduction in the EU legislation of collective redress mechanisms for breach of data protection rules. In particular, collective redress mechanisms empowering groups of citizens to combine their claims in a single action might constitute a very powerful tool to facilitate the enforcement of the data protection rules.⁴² This innovation is also supported by the Data Protection Authorities in the WP document on the Future of Privacy.

96. In cases with smaller impact, it is unlikely that the victims of a breach of data protection rules would bring individual actions against the controllers, given the costs, delays,

⁴⁰ Consent is usually linked to the age when children can enter into contractual obligations. This is the age when children are supposed to have reached a certain level of maturity. For example, Spanish law requires parental consent to collect children data for children who are not yet 14 years old. Above this age, children will be deemed to be able to consent. In the United Kingdom, the Data protection Act does not refer to a particular age or threshold. However, the UK Data protection Authority has interpreted that children **above 12** can provide consent. Conversely, children under **12** cannot provide consent and in order to obtain their personal data first it is necessary to obtain the permission of a parent or guardian.

⁴¹ In the US, COPPA requires operators of commercial websites or online services directed to children under 13 to obtain parental consent before collecting personal information and operators of commercial general audience websites to have actual knowledge that specific visitors are children.

⁴² See also EDPS Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 10.

uncertainties, risks and burdens they would be exposed to. These difficulties could be overcome or substantially alleviated if a system of collective redress were in place, empowering the victims of breaches to bundle their individual claims in a single action. The EDPS would also favour the empowerment of qualified entities, such as consumer associations or public bodies, to bring actions for damages on behalf of victims of data protection breaches. These actions should be without prejudice to the right of data subject to bring individual actions.

97. Not only are collective actions important for ensuring full compensation or other remedial action; they also perform indirectly a deterrence enhancing function. The risk of incurring expensive collective damages in such actions would multiply the controllers' incentives to effectively ensure compliance. In this regard, an enhanced private enforcement by means of collective redress mechanisms would complement public enforcement.
98. The Communication does not take a position regarding this topic. The EDPS is aware of the ongoing debate at European level on the introduction of consumer collective redress. He is also conscious of the risk of excesses that these mechanisms may bring about on the basis of the experience in other legal systems. However, these factors do not constitute in his view sufficient arguments to reject or postpone their introduction in the data protection legislation, in light of the benefits that they would entail⁴³.

7. Strengthening the role of organisations/controllers

7.1. General

99. The EDPS is of the opinion that, in addition to reinforcing individuals' rights, a modern legal instrument for data protection must contain the necessary tools that enhance the responsibility of data controllers. More particularly, the framework must contain incentives for data controllers in the private or public sector to pro-actively include data protection measures in their business processes. These tools would in the first place be helpful because, as said before, technological developments resulted in a sharp growth in the collection, use and further transfer of personal data which heightens the risks for the privacy and protection of personal data of individuals which should be compensated in an effective way. In the second place, the current framework lacks - except in a few, well-defined provisions (see below) - such tools and data controllers may take a *reactive* approach to data protection and privacy, and only act after a problem has arisen. This approach is reflected in statistics that show poor compliance practices and data losses as recurring problems.
100. According to the EDPS, the existing framework is not enough to protect personal data effectively under present and future conditions. The higher the risks, the higher the need to implement concrete measures that protect information at a practical level and deliver effective protection. Unless these pro-active measures are *de facto* implemented, mistakes, mishaps and negligence are likely to continue, endangering individuals' privacy in this increasingly digital society. To achieve this, the EDPS proposes the following measures.

7.2. Reinforcing data controllers' accountability

101. The EDPS recommends inserting a new provision in the legal instrument requiring data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the legal instrument and demonstrate this on request.

⁴³ Some national laws already provide for similar mechanisms.

102. This type of provision is not entirely new. Article 6 (2) of the Directive 95/46 refers to the principles relating to data quality and mentions that “It shall be for the controller to ensure that paragraph 1 is complied with”. Equally, Article 17 (1) requires data controllers to implement measures, of both a technical and organisational nature. However, these provisions have a limited scope. Inserting a general provision on accountability would stimulate controllers to put into place proactive measures in order to be able to comply with all the elements of data protection law.
103. A provision on accountability would have the consequence that data controllers are required to put in place internal mechanisms and control systems ensuring compliance with the principles and obligations of the framework. This would require, for example, involving the highest management in data protection policies, mapping procedures to ensure proper identification of all data processing operations, having binding data protection policies which should also be continually reviewed and updated to cover new data processing operations, complying with the principles of data quality, notice, security, access, etc. It would also require that controllers keep evidence to demonstrate compliance to authorities on request. Demonstrating compliance to the public at large should, in certain cases, also be made mandatory. This could be done for instance, by requiring controllers to include data protection in public (annual) reports, when such reports are mandatory on other grounds.
104. Obviously, the types of internal and external measures to be implemented must be appropriate and depend on the facts and circumstances of each particular case. It makes a difference whether a controller processes a few hundred customer records consisting merely of names and addresses or if he processes records of millions of patients, including their medical history. The same applies to the specific ways in which the effectiveness of the measures must be assessed. There is a need for scalability.
105. The general comprehensive data protection legal instrument should not lay down the specific requirements of accountability but only its essential elements. The Communication foresees certain elements to reinforce the responsibility of data controllers, which are very welcome. More particularly, the EDPS fully supports making data protection officers and privacy impact assessments mandatory, under certain threshold conditions.
106. Additionally, the EDPS recommends delegating powers to the Commission under Article 290 TFEU to supplement the basic requirements necessary to meet the accountability standard. Using these powers would enhance data controllers' legal certainty and harmonize compliance throughout the EU. In developing such specific instruments, the Article 29 Working Party and the EDPS should be consulted.
107. Finally, the concrete accountability measures to be implemented by data controllers could also be imposed by data protection authorities in the context of their enforcement powers. To do so, data protection authorities should be given new powers enabling them to impose remedial measures or sanctions. Examples should include setting up internal compliance programs, to implement privacy by design in specific products and services, etc. Remedies should only be imposed in so far as they are appropriate, proportionate and effective to ensure compliance with applicable and enforceable legal standards.

7.3. Privacy by design

108. Privacy by design refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data. According to the EDPS privacy by design is an element of accountability. Accordingly, data controllers would also be required to demonstrate that they had implemented privacy by design, where appropriate. Recently, the 32nd International Conference of Data Protection and Privacy Commissioners issued a resolution recognising privacy by design as an essential component of fundamental privacy protection.⁴⁴
109. Directive 95/46 contains some provisions encouraging privacy by design⁴⁵, but does not recognize such obligation explicitly. The EDPS is pleased with the Communication's endorsement of privacy by design as a tool towards ensuring compliance with the data protection rules. He suggests including a binding provision setting forth a "privacy by design" obligation, which could build on the wording of Recital 46 of Directive 95/46. More specifically, the provision would explicitly require data controllers to implement technical and organization measures, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to ensure the protection of personal data and prevent any unauthorized processing.⁴⁶
110. On the basis of such a provision data controllers would be required - inter alia - to ensure that data processing systems are designed to process as little personal data as possible, to implement privacy by default settings, for example in social networks, to keeping individual's profiles private from others by default and to implement tools enabling users to better protect their personal data (e.g. access controls, encryption).
111. The advantages of a more explicit reference to privacy by design can be summarised as follows:
- It would highlight the importance of the principle *per se*, as a tool towards ensuring that processes, products and services are designed from the outset with privacy in mind.
 - It would reduce privacy abuses and it would minimize the unnecessary collection of data and empower individuals to exercise real choices as their personal data.
 - It would avoid having to put "band aids" later on in an attempt to fix problems that may be difficult to repair if not impossible.
 - it would also facilitate the effective application and enforcement of this principle by data protection authorities.
112. The combined effect of this obligation would result in a stronger demand for privacy by design products and services, which should give more incentives to industry to meet such demand. It should be considered, on top of that, to create a separate obligation addressed to designers and manufacturers of new products and services with likely impact

⁴⁴ Resolution on Privacy by Design, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem 27-29 October 2010.

⁴⁵ The Directive includes provisions which indirectly, in different situations, demand the implementation of privacy by design. In particular, Article 17 requires that data controllers implement appropriate technical and organization measures to prevent unlawful data processing. The ePrivacy Directive is more explicit. Article 14.3 provides that "*Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications*".

⁴⁶ Under the present framework, Recital 46 encourages controllers implementing such measures, but a recital does of course not have binding force.

on data protection and privacy. The EDPS suggests including such a separate obligation which could further enable data controllers to comply with their own obligation.

113. The codification of privacy by design could be complemented by a provision setting forth general privacy by design requirements applicable across sectors, products and services, such as for example, ensuring user's empowerment measures, to be adopted pursuant to the principle.
114. Additionally, the EDPS recommends delegating powers to the Commission under Article 290 TFEU to - where appropriate - supplement the basic requirements of privacy by design for selected products and services. Using these powers would enhance data controllers' legal certainty and harmonize compliance throughout the EU. In developing such specific instruments, the Article 29 Working Party and the EDPS should be consulted (see in the same way point 106 on accountability).
115. Finally, the data protection authorities should be given the power to impose remedial measures or sanctions, under similar restrictive conditions as already mentioned in point 107, where controllers have clearly failed to take concrete steps in cases where this would be required.

7.4. Certification services

116. The Communication recognizes the need to explore the creation of EU certification schemes for privacy compliant products and services. The EDPS fully supports this aim and suggests including a provision providing for their creation and possible effect across the EU, which may be further developed later on in additional legislation. The provision should complement the provisions on accountability and privacy by design
117. Voluntary certification schemes would enable verification that a data controller has put in place measures to comply with the legal instrument. Furthermore, data controllers - or even products or services - enjoying the benefit of a certification label are likely to gain a competitive advantage over others. Such schemes would also help data protection authorities in their supervision and enforcement role.

8. Globalisation and applicable law

8.1. A clear need for more consistent protection

118. As mentioned earlier in Chapter 2, the transfer of personal data beyond the EU borders has exponentially grown as a consequence of the development of new technologies, the role of multinational companies and the increased influence of governments in the processing and sharing of personal data on an international scale. This is one of the main reasons justifying the revision of the current legal framework. Consequently, this is one of the areas where the EDPS asks for ambition and effectiveness, since there is a clear need for more consistent protection where data are processed outside the EU.

8.2. Investing in international rules

119. According to the EDPS more investment is needed in the development of international rules. More harmonisation with regard to the level of protection of personal data across the world would considerably clarify the substance of the principles to be complied with, and the conditions for transfers of data. These global rules would need to reconcile the

requirement for a high standard of data protection - including core EU data protection elements - with regional specificities.

120. The EDPS supports the ambitious work done so far in the framework of the International Conference of Data Protection Commissioners to develop and disseminate the so called "Madrid standards", with a view to integrate them into a binding instrument and possibly initiate an intergovernmental conference.⁴⁷ He calls on the Commission to take the necessary initiatives to facilitate the realisation of this objective.

121. In the view of the EDPS it is also important to ensure consistency between this initiative for international standards, the current review of the EU data protection framework and other developments such as the current revision of the OECD Privacy Guidelines and of Convention 108 of the Council of Europe which is open to signature by third countries (see also point 17). The EDPS considers that the Commission has a specific role to play here, in specifying how it will promote such consistency in the negotiations in the OECD and the Council of Europe.

8.3. Clarifying applicable law criteria

122. Since full consistency can not easily be achieved, there will - at least in the near future - remain some diversity between the laws within the EU and a fortiori beyond EU borders. The EDPS considers that a new legal instrument will need to clarify the criteria determining applicable law, and to ensure streamlined mechanisms for data flows as well as accountability of actors involved in data flows.

123. In the first place the legal instrument should ensure that EU law is applicable when personal data are processed outside the borders of the EU, but where there is a justified claim of applying EU law. The example of non European cloud computing services targeted to EU residents is an illustration why this is needed. In an environment where data are not physically stored and processed in a fixed location, where service providers and users located in different countries have interfering influence on data, it is very difficult to identify who is responsible for complying with which data protection principles. Guidance is being given, especially by data protection authorities, on how to interpret and apply Directive 95/46 in such cases, but guidance alone is not enough to ensure legal certainty in this new environment.

124. Within the territory of the EU the need for more precision in the legal framework and a simplified criterion to determine the law applicable has been emphasised by the Article 29 Working Party in a recent opinion.⁴⁸

125. According to the EDPS, the preferred option would be to lay down the legal instrument in a Regulation which would lead to identical rules applicable in all Member States. A regulation would make the need of determining applicable law less important. This is one of the reasons why the EDPS strongly favours the adoption of a Regulation. However, also a Regulation could allow some margin of manoeuvre for the Member States. If some significant margin of manoeuvre is kept in the new instrument, the EDPS would support the suggestion from the Working Party for a shift from a distributive application of different national laws to a centralised application of a single legislation in all Member States where a controller has establishments. He also pleads for more

⁴⁷ As suggested by Resolution on International Standards, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem 27-29 October 2010.

⁴⁸ WP29 Opinion 8/2010 on applicable law, WP 179

cooperation and coordination between Data Protection Authorities in transnational cases and complaints (see Chapter 10).

8.4. Streamlining mechanisms for data flows

126. The need for consistency and for a high level benchmark must be taken into account not only with a view to global data protection principles, but also with regard to international transfers. The EDPS fully supports the objective of the Commission to streamline current procedures for international data transfers and ensure a more uniform and coherent approach vis-à-vis third countries and international organisations.
127. The mechanism of data flows includes both private sector transfers, in particular via contractual clauses or Binding Corporate Rules (BCRs), and transfers between public authorities. BCRs are one of the elements where a more coherent and streamlined approach would be desirable. The EDPS recommends addressing conditions for BCRs in an explicit way in the new legal instrument⁴⁹, by:
- recognizing explicitly BCRs as tools that provide adequate safeguards;
 - providing for the main elements/ conditions for the adoption of BCRs;
 - setting forth cooperation procedures for the adoption of BCRs, including criteria for the selection of a leading supervisory authority (one stop shop).

9. The Area of police and justice

9.1. The general instrument

128. The Commission has repeatedly highlighted the importance of strengthening data protection in the context of law enforcement and crime prevention where the exchange and use of personal information has significantly intensified. Also the Stockholm Programme, approved by the European Council, refers to a strong data protection regime as the main prerequisite for the EU Information Management Strategy in this area.⁵⁰
129. The review of the general data protection framework is the perfect occasion to make progress in this respect, in particular since the Communication rightly describes Framework Decision 2008/977 as inadequate.⁵¹
130. The EDPS argued in section 3.2.5 of this Opinion why the area of police and judicial cooperation should be included in the general instrument. Inclusion of police and justice has a number of additional advantages. It means that the rules will no longer only apply to cross-border data exchanges⁵², but also to domestic processing. Adequate protection in the exchange of personal data with third countries will be better guaranteed, also with regard to international agreements. Furthermore, DPAs will have the same extensive and harmonised powers vis-à-vis police and judicial authorities as they have vis-à-vis other data controllers. Finally, the current Article 13, providing for the Member States' power to adopt specific legislation to restrict obligations and rights under the general instrument for specific public interests, will have to be applied in the same restrictive way as it applies in other areas. In particular, the specific safeguards provided for under the general

⁴⁹ On international transfers, see also Chapter 8 of the opinion.

⁵⁰ See on this EDPS Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice", paras 9-19.

⁵¹ See Section 3.2.5 above.

⁵² This is currently the limited scope of Framework Decision 2008/977.

instrument in this field will have to be respected also in national legislation adopted in the area of police and judicial cooperation.

9.2. Additional specific rules for police and justice

131. However, such an inclusion does not exclude special rules and derogations, which duly take account of the specificities of this sector, in line with Declaration 21 attached to the Lisbon Treaty. Limitations to the rights of data subjects may be foreseen, but they have to be necessary, proportionate and not alter the essential elements of the right itself. It should be emphasized in this context that Directive 95/46, including its Article 13, currently applies to law enforcement in various areas (e.g. taxation, customs, antifraud) that are not fundamentally different from many activities in the area of police and justice.

132. In addition, specific safeguards need also to be put in place, in order to compensate the data subject by giving him additional protection in an area where the processing of personal data may be more intrusive.

133. In light of the above, the EDPS considers that the new framework should include at least the following elements, in line with Convention 108 and Recommendation No R (87) 15:

- A distinction between different categories of data and files in accordance with their accuracy and reliability, endorsing the principle that data based on facts should be distinguished from data based on opinions or personal assessment.
- A distinction between various categories of data subjects (criminal suspects, victims, witnesses, etc.) and files (temporary, permanent and intelligence files). Specific conditions and safeguards need to be foreseen for the processing of data of non-suspects.
- Mechanisms to ensure periodic verification and rectification in order to safeguard the quality of the data being processed.
- Specific provisions and/or safeguards may be devised in relation to the (increasingly relevant) processing of biometric and genetic data in the field of law enforcement. Their use should be limited only to cases where no less intrusive means are available which may ensure the same effect.⁵³
- Conditions for transfers of personal data to non competent authorities and private parties, as well as for access and further use by law enforcement authorities of personal data collected by private parties.

9.3. Sector specific data protection regimes

134. The Communication states that "the Framework Decision does not replace the various sector-specific legislative instruments for police and judicial co-operation in criminal matters adopted at EU level, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), which either contain particular data protection regimes, and/or which usually refer to the data protection instruments of the Council of Europe".

135. In the view of the EDPS, a new legal framework should be, as far as possible, clear, simple and consistent. When there is a proliferation of different regimes applying to for instance Europol, Eurojust, SIS and Prüm, compliance with the rules remains or even

⁵³ In this direction, see WP document on the Future of Privacy, point 112.

becomes more complicated. That is one of the reasons why the EDPS favours a comprehensive legal instrument for all sectors.

136. However, the EDPS understands that aligning the rules from the different systems will require considerable work, which has to be carried out carefully. The EDPS considers that a gradual approach as mentioned in the Communication makes sense as long as the commitment to ensuring a high level of data protection in a consistent and effective way remains clear and visible. To be more concrete:
- In a first stage, the general legal instrument for data protection should be made applicable to all processing in the area of police and judicial cooperation, including the adjustments for police and justice (as meant in 9.2).
 - In a second stage, the sector specific data protection regimes should be aligned with this general instrument. The Commission should commit itself to adopt proposals for this second stage, within a short and specified timeframe.

10. DPAs and the Cooperation between DPAs

10.1. Reinforcing the role of DPAs

137. The EDPS fully supports the objective of the Commission to address the issue of the status of data protection authorities (DPAs), and more explicitly to strengthen their independence, resources and enforcement powers.
138. The EDPS also insists on the need to clarify in the new legal instrument the essential notion of independence of DPAs. The European Court of Justice has recently taken a decision on this issue in Case C-518/07⁵⁴, where it emphasised that independence means the absence of any external influence. A DPA may seek nor take instructions from anybody. The EDPS suggests explicitly codifying these elements of independence in the law.
139. In order to exercise their tasks the DPAs must be given sufficient human and financial resources. The EDPS suggests including this requirement in the law.⁵⁵ He finally stresses the need to make sure that authorities have fully harmonised powers in terms of investigation and imposing sufficiently deterring and remedial measures and sanctions. This would enhance legal certainty for data subjects and for data controllers.
140. Strengthening the independence, resources and powers of DPAs should go together with reinforced cooperation at multilateral level, especially in view of the growing number of data protection issues on a European scale. The main infrastructure to be used for this cooperation is obviously the Article 29 Working Party.

10.2. Strengthening the role of the Working Party

141. History shows that, from its start in 1997 until today, the functioning of the group has evolved. It has grown towards more independence and may not qualify any more, in practice, as a simple advisory working party to the Commission. The EDPS suggests further improvements of the functioning of the Working Party, including of its infrastructure and its independence.

⁵⁴ Case C-518/07, *Commission v. Germany*, not yet published in ECR.

⁵⁵ See, for example Article 43 (2) of Regulation 45/2001, which contains such requirement for the EDPS.

142. The EDPS believes that the strength of the group is intrinsically linked with the independence and powers of its members. The autonomy of the Working Party should be ensured in the new legal framework, in accordance with the criteria developed for a complete independence of DPAs by the European Court of Justice in case C-518/07. The EDPS considers that the Working Party should also be provided with sufficient resources and budget and a reinforced secretariat, to support its contributions.

143. With regard to the secretariat of the Working Party, the EDPS values the fact that it is integrated in the Data Protection Unit of DG Justice, with the advantage that the Working Party itself can benefit from efficient and flexible contacts and up-to-date information on data protection developments. On the other hand, he questions the fact that the Commission (and more specifically the Unit) is at the same time member, secretariat and addressee of the Working Party's opinions. This would justify more independence of the secretariat. The EDPS encourages the Commission to assess - in close consultation with stakeholders - how this independence can best be ensured.

144. Finally, reinforcing the powers for DPAs also requires stronger powers for the Working Party, with a structure including better rules and safeguards and more transparency. This will be developed for the advisory role as well as for the enforcement role of the Working party.

10.3. The advisory role of the Working Party

145. The positions of the Working Party must be effectively implemented when it comes to its advisory role to the Commission, especially in relation to the interpretation and application of the principles of the Directive and other data protection instruments, in other words to ensure the authoritative character of the Working Party positions. Further discussion is needed amongst DPAs in order to identify how to include this in the legal instrument.

146. The EDPS recommends solutions which would make opinions of the Working Party more authoritative without modifying substantially its way of functioning. The EDPS suggests including an obligation for the DPAs and the Commission to *take utmost account of opinions and common positions* adopted by the Working Party, based on the model adopted for the positions of the Body of European Regulators for Electronic Communications (BEREC)⁵⁶. Furthermore, the new legal instrument could give the Working Party the explicit task to adopt “interpretative recommendations”. These alternative solutions would give the positions of the Working Party a stronger role, also before the Courts.

10.4. Coordinated enforcement by the Working Party

147. Under the present framework the enforcement of data protection law in the Member States is left to 27 Data Protection Authorities with little coordination as regards the handling of specific cases. When it comes to cases involving more than one Member State or having clearly a global dimension, this multiplies costs for undertakings, which are forced to deal with different public authorities for the same activity, and it enhances the risk of inconsistent application: in exceptional cases, the same processing activities may be considered lawful by one DPA and prohibited by another.

⁵⁶ Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L337, 9 18.12.2009, p. 1.

148. Some cases have a strategic dimension which should be addressed in a centralised way. The Article 29 Working Party facilitates coordination and enforcement actions between DPAs⁵⁷ in major data protection issues with such international implications. This was the case with social networks and search engines⁵⁸, as well as with regard to coordinated inspections conducted in different Member States on telecommunication and health insurance issues.

149. There are however limits to the enforcement actions that the Working Party can undertake under the present framework. Common positions can be taken by the Working Party, but there is no instrument to ensure that these positions are effectively implemented in practice.

150. The EDPS suggests including in the legal instrument additional provisions that could support coordinated enforcement, in particular:

- An obligation to ensure that DPAs and the Commission *take utmost account of opinions and common positions* adopted by WP 29.⁵⁹
- An obligation for DPAs to faithfully cooperate with each other and with the Commission and the WP 29⁶⁰. As a practical illustration of a faithful cooperation, a procedure could be set up by which DPAs inform the Commission or the Working Party in case of national enforcement measures with a cross border element, in analogy to the procedure applicable in the present framework with regard to national adequacy decisions.
- Specifying the voting rules to increase the commitment of DPAs to implement the decisions of the Working Party. It could be provided that the Working Party envisages deciding on the basis of consensus and when consensus could not be reached takes enforcement only with a qualified majority. In addition to this, a recital could foresee that those DPAs casting a positive vote on a document have an obligation or policy commitment to implement it at national level.

151. The EDPS would put a caveat against introducing stronger measures, such as giving binding force to WP29 positions. This would undermine the independent status of individual DPAs, which has to be guaranteed by the Member States under national law. Would the Working Party decisions have a direct impact on third parties such as data controllers, new procedures should be foreseen including safeguards such as transparency and redress, including possibly appeal before the European Court of Justice.

10.5. Cooperation between the EDPS and the Working Party

152. The way in which the EDPS and the Working Party cooperate could also be fine-tuned. The EDPS is a member of the Working Party, and he contributes within the group to positions on the main strategic EU developments, while ensuring consistency with his own positions. The EDPS notes the increasing number of privacy issues, both in the private as well as in the public sector, which have implications at national level in many Member States, and where there is a specific role for the Working Party to play.

⁵⁷ Beside the Article 29 Working Party, the European Conference of Data Protection Commissioners has created about ten years ago a permanent workshop aimed at addressing cross-border complaints in a coordinated way. Although this workshop presents undeniable added value in terms of exchange between DPAs' staffs and offers a reliable network of contact points, it can not be considered as a coordination mechanism for decision making.

⁵⁸ See the letters of WP 29 of 12.05.2010 and 26.05.2010, published on the WP29 website (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

⁵⁹ As mentioned above, a similar obligation is laid down in Regulation (EC) No 1211/2009 which specifies the role of the Body of European Regulators for Electronic Communications (BEREC)..

⁶⁰ See, in this regard, Article 3 of Regulation (EC) No 1211/2009, cited above.

153. The EDPS has a complementary task to advise on the developments in the context of the EU, which should be maintained. As a European body, he exercises this advisory competence towards EU Institutions in the same way as national DPAs advise their governments.

154. The EDPS and the Working Party act from a different but complementary perspective. There is for these reasons a need to preserve and maybe improve coordination between the Working Party and the EDPS, to make sure that they work together on the main data protection issues, for instance by coordinating agendas on a regular basis⁶¹, and by ensuring transparency on issues which have a more national or specific EU aspect.

155. Coordination is not mentioned in the present Directive for the simple reason that the EDPS did not exist at the time where the Directive was adopted, but after six years of existence the complementarities of the EDPS and the Working Party are visible and could be formally recognised. The EDPS recalls that under Regulation 45/2001 he has the duty to cooperate with the national DPAs and to participate in the activities of the Working Party. The EDPS recommends to explicitly mention cooperation in the new legal instrument, and to structure it where necessary, for instance by laying down a procedure for cooperation.

10.6. Cooperation between the EDPS and the DPAs in supervision on EU systems

156. These considerations also apply to areas where the supervision must be coordinated between the European and national level. This is the case for EU bodies that process significant amounts of data delivered by national authorities or for large scale information systems with a European and a national component.

157. The existing system for some EU bodies and large scale information systems - for instance, Europol, Eurojust and the first generation Schengen Information System (SIS) have Joint Supervisory Bodies with representatives of national DPAs - is a remnant of intergovernmental cooperation in the pre-Lisbon era and does not respect the institutional structure of the EU of which Europol and Eurojust are now an integral part, and in which the "Schengen acquis" has now also been integrated⁶².

158. The Communication announces that the Commission will launch in 2011 a consultation of stakeholders on the revision of these supervision systems. The EDPS urges the Commission to take as soon as possible (within a short and specified timeframe, see above) position in the ongoing discussion on supervision. He will take - in this discussion - the following viewpoint.

159. As a point of departure, it should be guaranteed that all supervisory bodies fulfil the indispensable criteria of independence, resources and enforcement powers. Furthermore, it should be ensured that the perspectives and expertise that exists on the EU level is taken into account. That means that cooperation should take place not only between the national authorities but also with the European DPA (currently the EDPS). The EDPS finds it necessary to follow a model that fulfils these requirements.⁶³

⁶¹ E.g. on the basis of the Inventory of legislative activities published annually and updated regularly, which is available on the EDPS website.

⁶² Under Regulation 45/2001, the EDPS has a duty to cooperate with these bodies.

⁶³ For Eurojust, a model should also take into account that the data protection supervision respects the independence of the judiciary, in so far as Eurojust process data in the context of criminal proceedings.

160. In recent years the model of "coordinated supervision" was developed. This model of supervision, as now operational in Eurodac and parts of the Customs Information System, will soon be expanded to the Visa Information System (VIS) and the second generation Schengen Information System (SIS II). This model has three layers: (1) supervision at national level is ensured by DPAs; (2) supervision at EU level is ensured by the EDPS; (3) coordination is ensured by way of regular meetings convened by the EDPS acting as the secretariat of this coordination mechanism. This model has proven to be successful and effective and should be envisaged in the future for other information systems.

C. HOW TO IMPROVE APPLICATION OF PRESENT FRAMEWORK?

11. The short term

161. Whilst the review process is ongoing, efforts should be devoted to ensure full and effective implementation of the current rules. These rules will still be applicable until the future framework is adopted and then implemented into national laws of the Member States. In this direction, several lines of actions may be identified.

162. First, the Commission should continue monitoring Member States compliance with Directive 95/46 and, where necessary, use its powers under Article 258 TFEU. Recently, infringement proceedings have been opened for a failure to correctly implement Article 28 of the Directive with regard to the requisite of independence of DPAs⁶⁴. Also in other areas full compliance needs to be monitored and enforced.⁶⁵ The EDPS thus welcomes and fully supports the Commission's commitment in the Communication to pursue an active infringement policy. The Commission should also continue the structural dialogue with Member States on implementation.⁶⁶

163. Second, enforcement at national level must be encouraged so as to ensure practical application of data protection rules, including with respect to new technological phenomena and global players. DPAs should make full use of their investigative and sanctioning powers. It is also important that the existing rights of data subjects, particularly the rights of access, are fully implemented in practice.

164. Third, greater coordination in the enforcement seems necessary in the short term. The role of the WP29 and its interpretative documents in this regard is crucial, but also DPAs should do their most to put them in practice. Diverging outcomes in EU-wide or global cases need to be avoided and common approaches can and should be reached within the Working Party. EU-wide coordinated investigations under the auspices of the Working Party can also bring significant added value.

165. Fourth, data protection principles should be "built-in" proactively in new regulations which may have an impact, directly or indirectly, on data protection. At the EU level, the EDPS makes considerable efforts to contribute to better European legislation and these efforts must be undertaken also at national level. Data protection authorities should therefore make full use of their advisory powers to ensure such a proactive approach. Data protection authorities, including the EDPS, can also play a proactive role in monitoring technological developments. Monitoring is important with a view to identifying at an

⁶⁴ See Case C-518/07, cited above and Commission Press Release of 28 October 2010 (IP/10/1430).

⁶⁵ The Commission has opened an infringement proceeding against the UK for an alleged breach of various data protection provisions, including the requirement of confidentiality of electronic communications in respect of behavioural advertising. See Commission Press Release of 9 April 2009 (IP/09/570).

⁶⁶ See Commission's First Report on the implementation of the Data Protection Directive, cited above, p. 22 et seq.

early stage emerging trends, highlighting possible data protection implications, supporting data protection-friendly solutions and raising the awareness of stakeholders.

166. Finally, further cooperation between the various actors at international level needs to be actively pursued. It is therefore important to reinforce the international instruments of cooperation. Initiatives like the Madrid standards and the ongoing work within the Council of Europe and the OECD deserve full support. In this context, it is very positive that also the US Federal Trade Commission has now joined the family of Privacy and Data Protection Commissioners in the framework of their International Conference.

D. CONCLUSIONS

General observations

167. The EDPS welcomes the Commission's Communication in general, as he is convinced that the review of the present legal framework for data protection is necessary, in order to ensure effective protection in an increasingly developing and globalised information society.

168. The Communication identifies the main issues and challenges. The EDPS shares the view of the Commission that a strong system of data protection will still be needed in the future, based on the notion that existing general principles of data protection are still valid in a society which undergoes fundamental changes. The EDPS shares the statement in the Communication that the challenges are enormous and underlines the consequence that the proposed solutions should be correspondingly ambitious and enhance the effectiveness of the protection. As a result he asks for a more ambitious approach on a number of points.

169. The EDPS fully supports the comprehensive approach to data protection. However, he regrets that the Communication excludes certain areas, such as the data processing by EU institutions and bodies, from the general legal instrument. If the Commission were to decide to leave out these areas, the EDPS urges the Commission to adopt a proposal for the EU level within the shortest possible timeframe, but preferably by the end of 2011.

Main perspectives

170. The points of departure of the review process for the EDPS are as follows:
- Arrangements for data protection must as far as possible actively support rather than hamper other legitimate interests (such as European economy, the security of individuals and accountability of governments).
 - The general principles of data protection should not and cannot be changed.
 - Further harmonisation should be one of the key objectives of the review.
 - The fundamental rights perspective should lie at the heart of the review process. A fundamental right aims to protect citizens under all circumstances.
 - The new legal instrument must include the police and justice sector.
 - The new legal instrument must be formulated in a technologically neutral way as much as possible and must aim to create legal certainty over the longer term.

Elements of a new framework

Harmonisation and simplification

171. The EDPS welcomes the Commission's commitment to examine the means to achieve further harmonisation of data protection at EU level. The EDPS determines areas where further and better harmonisation is urgent: definitions, grounds for data processing, data subjects' rights, international transfers and data protection authorities.

172. The EDPS suggests considering the following alternatives to simplify and/or reduce the scope of the notification requirements:

- Limit the obligation to notify to specific kinds of processing operations entailing specific risks.
- A simple registration obligation requiring data controllers to register (as opposed to extensive registration of all data processing operations).
- The introduction of a standard pan-European notification form.

173. According to the EDPS a Regulation, a single instrument which is directly applicable in the Member States, is the most effective means to protect the fundamental right to data protection and to achieve further convergence in the internal market.

Strengthening the rights of individuals

174. The EDPS supports the Communication where it proposes strengthening individuals' rights. He makes the following suggestions:

- A principle of transparency could be included in the law. However, it is more important to reinforce the existing provisions dealing with transparency (such as the existing Articles 10 and 11 of Directive 95/46).
- A provision on personal data breach notification, which extends the obligation included in the revised ePrivacy Directive from certain providers to all data controllers, should be introduced in the general instrument.
- The limits of consent should be clarified. Broadening the cases where express consent is required should be considered as well as adopting additional rules for the online environment.
- Additional rights should be introduced such as data portability and the right to be forgotten, especially for information society services on the internet.
- Children's interests should be better protected with a number of additional provisions, specifically addressed to the collection and further processing of children's data.
- Collective redress mechanisms for breach of data protection rules should be introduced in the EU legislation, in order to empower qualified entities to bring actions on behalf of groups of individuals.

Strengthening the obligations of organisations/controllers

175. The new framework must contain incentives for data controllers to pro-actively include data protection measures in their business processes. The EDPS proposes the introduction of general provisions on accountability and "privacy by design". A provision on privacy certification schemes should also be introduced.

Globalisation and applicable law

176. The EDPS supports the ambitious work in the framework of the International Conference of Data Protection Commissioners to develop the so called "Madrid standards", with a view to integrate them into a binding instrument and possibly initiate an intergovernmental conference. The EDPS calls on the Commission to take concrete steps in this direction in close cooperation with the OECD and the Council of Europe.

177. A new legal instrument must clarify the criteria determining applicable law. It should be ensured that data that are processed outside the borders of the EU do not escape EU jurisdiction where there is a justified claim for applying EU law. If the legal framework would have the form of a Regulation there would be identical rules in all Member States and it would become less relevant to determine applicable law (within the EU).

178. The EDPS fully supports the objective to ensure a more uniform and coherent approach vis-à-vis third countries and international organisations. Binding Corporate Rules (BCRs) should be included in the legal instrument.

The area of police and justice

179. A comprehensive instrument including police and justice may allow for special rules which duly take account of the specificities of this sector, in line with Declaration 21 attached to the Lisbon Treaty. Specific safeguards need to be put in place, in order to compensate data subjects by giving them additional protection in an area where the processing of personal data is by nature more intrusive.

180. The new legal framework should be, as far as possible, clear, simple and consistent. A proliferation of different regimes applying to, for instance, Europol, Eurojust, SIS and Prüm, should be avoided. The EDPS understands that aligning the rules from the different systems will have to be carried out carefully and gradually.

DPAs and the cooperation between DPAs

181. The EDPS fully supports the objective of the Commission to address the issue of the status of data protection authorities (DPAs), and to strengthen their independence, resources and enforcement powers. He recommends:

- Codifying in the new legal instrument the essential notion of independence of DPAs, as specified by the ECJ.
- Stating in the law that DPAs must be given sufficient resources.
- Giving authorities harmonised investigation and sanctioning powers.

182. The EDPS suggests further improvements of the functioning of the Article 29 Working Party, including its independence and infrastructure. The Working Party should also be provided with sufficient resources and a reinforced secretariat.

183. The EDPS suggests reinforcing the advisory role of the Working Party by introducing an obligation for DPAs and the Commission to *take the utmost account of opinions and common positions* adopted by the Working Party. The EDPS is not in favour of giving binding force to Working Party positions, particularly because of the independent status of individual DPAs. The EDPS recommends that the Commission introduce specific provisions to enhance cooperation with the EDPS in the new legal instrument.

184. The EDPS urges the Commission to take a position as soon as possible on the issue of supervision of EU bodies and large scale information systems, taking into consideration that all supervisory bodies should fulfil the indispensable criteria of independence, sufficient resources and enforcement powers and that it should be ensured that the EU perspective is well represented. The EDPS supports the model of 'coordinated supervision'.

Improvements under the present system:

185. The EDPS encourages the Commission to:

- Continue monitoring Member States' compliance with Directive 95/46 and, where necessary, using its enforcement powers under Article 258 TFEU.
- Encourage enforcement at the national level and the coordination of enforcement.
- Build data protection principles pro-actively into new regulations which may have an impact, directly or indirectly, on data protection.
- Actively pursue further cooperation between the various actors at international level.

Brussels, 14 January 2011

(signed)

Peter HUSTINX
European Data Protection Supervisor



Ethical aspects of information and communication technologies



Lee HIBBARD

Coordinator on the information society and Internet governance, Council of Europe

Lee Hibbard is the Head of the Information Society Unit at the Council of Europe in the Directorate-General of Human Rights and Rule of Law.

Over the last four years he has coordinated the work of the Council of Europe (<http://www.coe.int>) in various international forums dealing with the information society and Internet governance, in particular the European Dialogue on Internet Governance (<http://www.eurodig.org>), the Internet Governance Forum (IGF) and the Governmental Advisory Committee of the Internet Corporation for Assigned Names and Numbers (ICANN).

At the substantive level, he has been heavily involved in the conception and development of several pan-European policy documents concerning empowerment of children online, the public service value of the Internet, protecting the dignity, security and privacy of children on the Internet, freedom of expression and Internet filters, as well as human rights guidelines for ISPs and online games providers.

As a consequence of his skills in transversal working methods, Lee is also involved in collaborative work between the Council of Europe and external partners, including HEC Montreal, on the future of management and communities of practice.



Council of Europe
Media and Information Society



Ethics in the information society Roundtable

What society do we want?

Brussels, 15 November 2011

Lee Hibbard,
Information Society Division, Council of
Europe: lee.hibbard@coe.int



Council of Europe
Media and Information Society



- Singing same song for freedom, and security provided it does not unduly threaten freedom
- HRs is the common core: shared, incumbent on us all to protect and respect, already 'bought into'
- We need to more: CoE-EC, Private Sector, Civil society, technical communities, IGOs, etc.
- CoE Strategy on IG 2012-2015



Ethics as a transmitter of human rights

- Ethics is the transmission of human rights and fundamental freedoms
- States protect, companies should respect, individuals responsible
- Access to info, knowledge and social interaction = coping
- Expected to appropriate skills, to self-determination, respect for others, to protect oneself
- Disengaged, disembodied?
- **CoE: bridging top-down morals with bottom-up ethics (multi-stakeholder dialogue catalyst)**
- **IG Principles patchwork – decentralised vs centralised**



CoE Origins & Facts

- **Inter-governmental** organisation
- 47 member state governments / 800 million
- International law / legally binding / European Court of Human Rights - governments held in violation
 - 2001 Budapest Covention on Cybercrime
 - 1981 Convention 108 on data protection (modernised, privacy by deisgn)
 - 2008 HRs guidelines' for ISPs and games providers
 - CoE Strategy on IG 2012-2015 (partnership)



State protecting and ensuring respect for human rights, rule of law, democracy

“High Contracting Parties **shall secure** to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention (...)”

Article 1, ECHR



More freedom, more ethics

“Everyone has the **right** to freedom of expression (...) freedom to hold opinions and to receive and impart information and ideas without interference (...) and regardless of frontiers.

(...) carries with it duties and ***responsibilities** (...)”

Article 10, ECHR / 500+ cases!

*ICANN



Technology fast, law slow
incumbent to be ethical when the
Internet is a global public resource

2 billion+ Internet users
worldwide

700 million Facebook

billions of YouTube
downloads (video/copyright)

6 billion mobile registrations
(mobile Internet 3G?)

Infrastructure: new gTLDs
(e.g. .xxx, .bank, .pharma
cy, etc)



ethics of states and intermediaries in the information society?

France (Hadopi)

Turkey (YouTube/defamation)

Italy (Google/privacy)

Is privacy "no longer a contemporary concept" for people in the 21st century?

Protecting children's 'right to be forgotten'



Ethical interpretations and responsibilities of states

- Clinton keynotes 2010/2011
- Sweden Internet freedom / UN
- USG grant to BBC World Service (outsourcing, not regulating)
- G8
- London Cyberconference (Hague statements)
- CoE Vienna HRs on Internet conference
- NL (US) Ministerial conference



IGO work on ethics

WSIS Action Line C10

- [values and principles] equality, solidarity, tolerance, *shared responsibility
- [responsibility] Awareness of ethical use of ICTs
- [protection] Protect privacy/personal data
- [protection] Combat abusive use of ICTs



UNESCO IFAP

- [HRs] Public **service** of Internet to exercise HRs
- [HRs/FoE] **Access to enable**: produce, communicate, innovate ... info/knowledge/creativity/participation, linguistic, cultural, social, educational
- [HRs/right to assembly] Freedom of **association** – no monitoring or surveillance
- **Trust**: technical **assurances** (CiR security, reliability, stability) + **literacy** (technical and media) + **privacy & security**



IG word cloud

ethical implications for different stakeholder groups

- Trust
- Freedom
- Protection
- Responsibility
- Security
- Openness
- Privacy
- Public service value
- Transparency
- Accountability

- **Need ethics for cloud, 'Internet of Things', etc**



• **CoE responses?**

shaping our ETHICAL understanding about the Internet/ ICTs



CoE 2009 Ministerial Conference (Reykjavik, 2009)

What freedom to CONNECT, control and manage our IDENTITIES...to **what extent should the onus be on the user?**

Who owns your data?

Information, transparency
& consent

Where do you turn to for accurate and trusted information? (Public service media **governance**)

Online right to reply and effective redress for **individuals (control)**

Does “delete” really delete?



Reliance, dependance, expectation...

People’s **significant reliance on the Internet** as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions, leisure) and the resulting **legitimate expectation** that a minimum level of core Internet services are **accessible and affordable, secure, reliable and ongoing**

CoE Recommendation on public service value of the Internet, 2007



(ethical processes) Bottom-up multi-stakeholder dialogue policy making

“Users should have the **greatest possible access** to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice (...)

(...) exceptions to this principle should be considered with great **circumspection and need to be justified by overriding public interests.**

“(...) **able to gauge** the impact of network management measures on the enjoyment of fundamental rights and freedoms (...). Those **measures should be proportionate, appropriate and avoid unjustified discrimination...**

CoE Recommendation on Network Neutrality, 2010



2011 CoE standards and guidelines

New notion of media indicators: editorial control/oversight, purpose, intent, outreach, professional standards, third party expectation

Critical Internet Resources: preparedness, avoiding disruption, “do no (transboundary) harm”



CoE Messages

- Maximising rights and services
- Minimising restrictions
- Ensuring level of security that users are entitled to expect



CoE 2012

- **search engine provider guidelines:** transparency, pluralism & diversity of sources of information, consent
 - **social network provider guidelines:** transparent info to users about DP management default settings, deleting profiles & content, anonymity-pseudonymity, reporting, 'opt-in' for wider access, easy controls to restrict
- * **CoE Internet governance strategy 2012-2015**
- **users charter** to complain, seek redress, recourse, right to reply, remedies
 - **ethics of ICT private sector - implementing** of UN SRSG John Ruggie Report



Mapping Ethical principles CoE IG Principles Declaration, Sep 2011

1. Human rights, democracy and the rule of law / all should uphold
2. Multi-stakeholder governance / full participation
3. Responsibilities of states / responsibility to refrain from harm and restricting rights
4. Empowerment of Internet users / participate
5. Universality of the Internet / should not misuse or interfere with traffic
6. Integrity of the Internet / security, stability, resilience
7. Decentralised management / private sector responsibility for day-to-day
8. Architectural principles / open, end-to-end, no barriers, no burdens
9. Open network / user access to choice in content, apps and services
10. Cultural and linguistic diversity / user freedom of expression



Personal ethical learnings inclusiveness, rights, freedoms, values

- Ethics is much about protecting users rights and freedoms
- State protecting, private sector respecting, individuals respecting
- More individual freedom – more expectations – more (unrealistic?) responsibilities
- Information, awareness (benefits/risks), literacy, tools = skills, competences, empowerment
- 'Best (individual) efforts'? and shared responsibilities to protect users as citizens and consumers (blurring of sectors)
- Multi-stakeholder ethics = a multiplicity of dialogues, joint signing-off of policies, deeper & wider consultation



Council of Europe

Media and Information Society



Thank you 😊

Lee Hibbard, Council of Europe,
Information Society Division, Council of
Europe: lee.hibbard@coe.int



Ethical aspects of information and communication technologies



Michele BELLAVITE

Chairman of the Digital Society Working
Group, European Telecommunications
Network Operators' Association (ETNO)

Michele Bellavite has worked since 2002 in the public and regulatory affairs division of Telecom Italia. Based in Brussels, he chairs the Digital Society Working Group of ETNO, and is also an alternate board member. He

holds a degree in political science from the University of Pavia, with a major in European political organisation, and has done postgraduate training at the College of Europe.

Digital society: an industrial perspective

Michele BELLAVITE

Roundtable on the Ethical Aspects of Information and Communication Technologies

TITLE:

Digital Society: an industrial perspective

NAME:

Michele Bellavite

ORGANISATION AND COUNTRY:

ETNO - Chairman of the Digital Society Working Group
Belgium

CONTENT OF THE PRESENTATION:

The telecommunications industry has recently been confronted with some new policy issues whereas before, the policy debate was largely focused on liberalization and access issues. This policy shift is, in part, due to fixed and mobile broadband investments by industry that have brought high speed Internet to a wider range of users and it is also due to the growing involvement of stakeholders in Internet policy debates, such as civil rights groups, law enforcement representatives and Governments.

The public policy debate on the Internet is increasingly centered on the relationship between the end-user and the on-line world / provider and indeed on appropriate behavior online. Many argue for the same level of protection afforded in the offline world to be applied in the online world. Telecom players are already committed to providing transparent and meaningful information regarding their offers and, in particular, any limitations on Internet access (eg speed throttling at 'high peak' times of the day), further strengthening consumer choice in this field. In addition, the telecoms regulatory framework offers numerous consumer protection safeguards, such as the contractual rights set out in the Citizens' Rights Directive. ETNO therefore believes that no further regulatory intervention is needed and that it is important to allow industry the freedom to innovate and adopt new business models and services in a fast moving technology environment. Indeed, it is the case that the telecoms sector is already over-burdened with sector-specific regulation that is not equally applied to other ICT players, such as over the top (OTT) players. As such, this regulatory asymmetry is damaging the telecoms sector and, at a broader level, it is damaging the competitive position of the EU.

In the context of the net neutrality debate, ETNO believes that existing regulatory provisions set forth in the Universal Service Directive offer adequate protection for consumers, while allowing telcos the ability to manage the huge growth in data traffic and make the Internet a more efficient and orderly place. Anti-competitive industry practices are naturally prohibited.

ETNO members do not exercise control over the actual content transmitted over their networks and do not engage in any form of censorship or seek to limit the right to freedom of expression. In

order to maintain an open Internet environment, the EU should maintain its current policies towards the protection of Internet intermediaries and not put them in the position of judging or monitoring content or communications.

Finally, as regards governance of the Internet, ETNO fully supports a multi stakeholder approach with no regulatory oversight by any one Government entity, considered that the challenges of Internet governance and principles are mainly around its global reach and nature. This collaborative, bottom up approach is fitting in view of the global nature of the Internet. The recent development and emergence of high level Internet principles (eg OECD Principles on Internet Economy, Aspen Principles for the Future of the Internet) is helpful in so far as setting forward best practice and guidelines for the online world. It would therefore be important that the EU start a reflection on how it can make sure that European values and human rights traditions can be safeguarded on a global level.



Ethical aspects of information and communication technologies



Bernd CARSTEN-STAHL

Professor of Critical Research in Technology
and Director of the Centre for Computing and
Social Responsibility, De Montfort University

Bernd Carsten-Stahl is Professor of Critical Research in Technology and Director of the Centre for Computing and Social Responsibility at De Montfort University, Leicester, UK. His interests cover philosophical issues arising from the intersections of business, technology and information. This includes the ethics of ICT and critical approaches to information systems. From 2009 to 2011

he served as coordinator of the EU seventh framework programme (FP7) research project on 'Ethical issues of emerging ICT applications' (ETICA) (<http://www.etica-project.eu>) and from 2012 to 2015 he will be coordinator of the FP7 research project 'Civil society organisations in designing research governance' (Consider) (<http://www.consider-project.eu>).

Ethics and future Internet

Bernd CARSTEN-STAHL



Emerging ICTs – Ethics and Governance

Bernd Carsten Stahl



The ETICA Project

1. Identify emerging ICTs
2. Identify ethical issues likely to be raised by those ICTs
3. Evaluate and rank these issues
4. Provide recommendations on appropriate governance structures to address these.



SIS 2008; GA 230318;
04/2009-05/2011

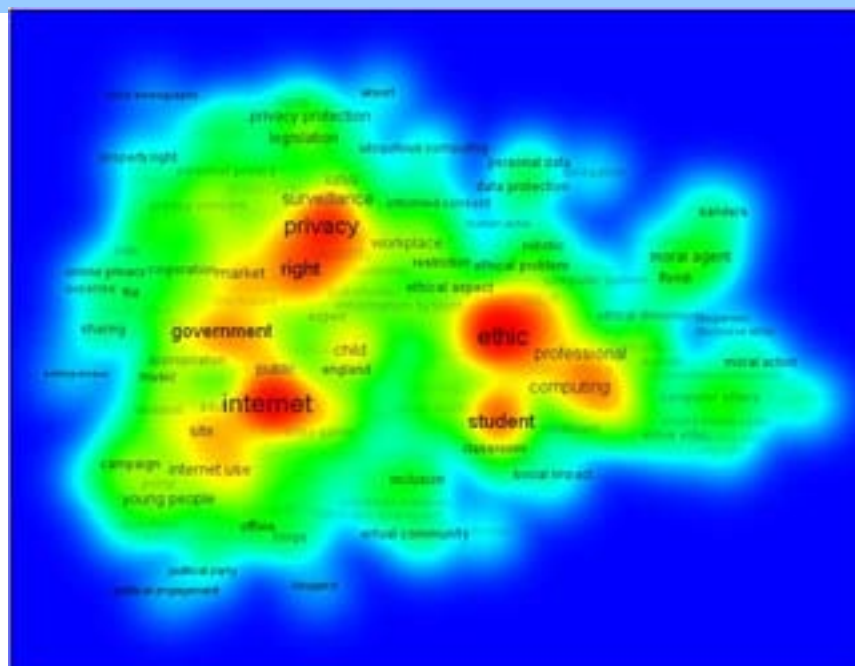
2

Emerging Technologies – Shared Features

- Natural interaction
- Invisibility
- Direct link
- Detailed understanding of the user
- Pervasiveness
- Autonomy
- Power over the user
- **Market driven**

3

Ethical Issues



4

Predictable Ethical Issues (examples)

- Privacy, but:
 - New types of data
 - New ways of linking data
 - New quantities of data
- Security
- Trust
- Liability
- Digital divides
(broadband is NOT the solution)

5

Less Obvious Ethical Issues (examples)

- View of humans
 - Therapy / enhancement
 - Normality
 - Mortality
 - Identity
- Power relationships
- Environment
- Nature of society
- Changing cultures

6

Governance Challenges

- Huge **number** of artefacts, application areas, interlinking systems
- Infinity of **moral** issues / diverging **ethical** evaluations
- Moral issues are **context** dependent
- Moral issues and preferences will **change** over time, are impossible to predict comprehensively
- Governance must be **flexible** and open to change and development
- Required: a combination of **ethical procedure** and **moral guidance**

7

ETICA Recommendations to Policy Makers

- **Provide regulatory framework which will support Ethical Impact Assessment for ICTs**
- **Establish an ICT Ethics Observatory**
- **Establish a forum for stakeholder involvement**

8

ETICA Recommendations for Industry and Researchers and CSOs

- **Incorporate ethics into ICT research and development**
- **Facilitate ethical reflexivity in ICT projects and practice**

9

The EGE Opinion on the Ethics of ICTs

- ICTs are more than just the Internet
- Ethics is more than just privacy
- The EGE Opinion needs to **open debate**, not close it
- EGE should aim to facilitate the **art of governance**

10



Ethical aspects of information and communication technologies



Guido VAN STEENDAM

Professor of the Philosophy of Technology, KU Leuven, and Director, International Forum for Biophilosophy

Guido Van Steendam is Professor of the Philosophy of Technology at the Higher Institute of Philosophy of the KU Leuven — University of Leuven (Belgium) and director of research at the International Forum for Biophilosophy.

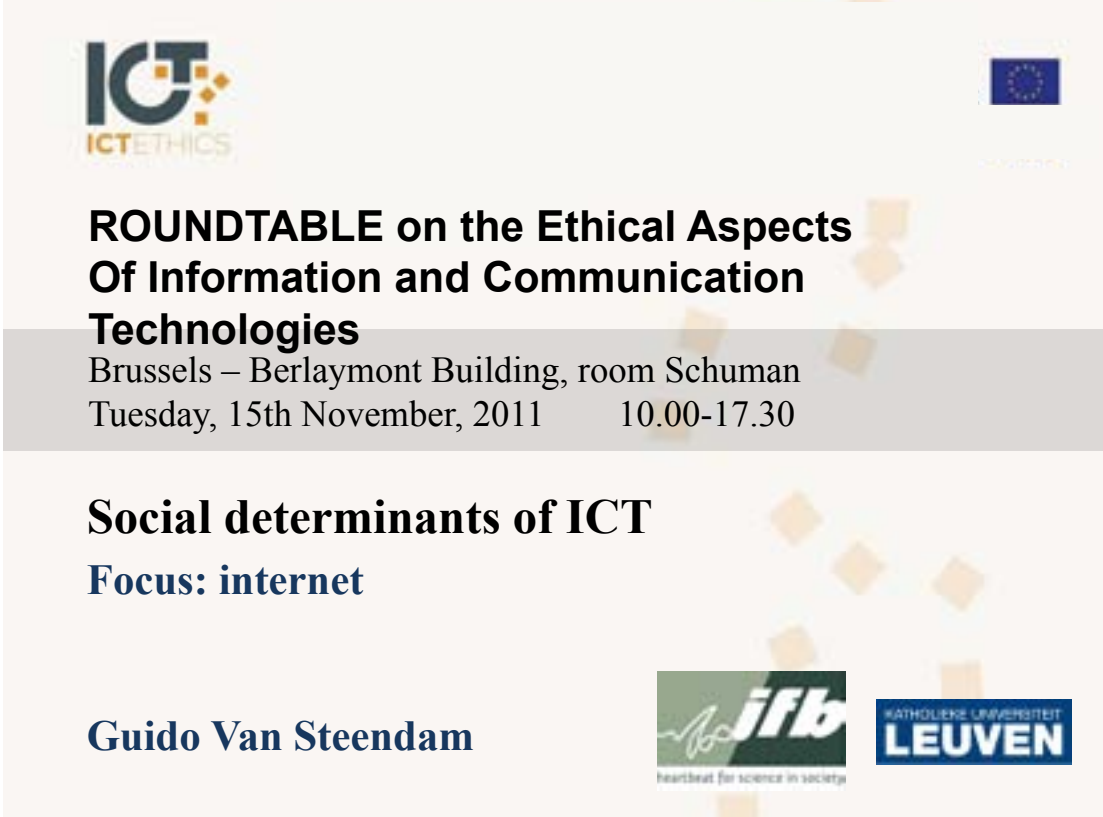
His research interests include the philosophy and ethics of biomedical developments (such as genetics, biotechnology, reproductive technologies, euthanasia and critical care medicine) as well as information and communication technologies (such as ambient intelligence, camera surveillance, social media) and converging

technologies. His research has two major components. An operational component is intended to clarify the work of engineers and politicians and others who are designing, analysing and regulating technology and is organised in close interaction with the actors involved. A methodological component reflects on the theoretical and institutional possibilities and limits to monitoring the development of science and technology.

Guido has an academic background in natural and human sciences, theology and philosophy.

Social determinants of ICT

Guido VAN STEENDAM



The poster features the ICTETHICS logo in the top left, the European Union flag in the top right, and a decorative pattern of orange squares. The main title is 'ROUNDTABLE on the Ethical Aspects Of Information and Communication Technologies'. The location and date are 'Brussels – Berlaymont Building, room Schuman' and 'Tuesday, 15th November, 2011 10.00-17.30'. The specific topic is 'Social determinants of ICT' with a focus on 'internet'. The speaker is 'Guido Van Steendam'. Logos for 'ifb' and 'KATHOLIEKE UNIVERSITEIT LEUVEN' are at the bottom right.

ICTETHICS

**ROUNDTABLE on the Ethical Aspects
Of Information and Communication
Technologies**

Brussels – Berlaymont Building, room Schuman
Tuesday, 15th November, 2011 10.00-17.30

Social determinants of ICT
Focus: internet

Guido Van Steendam

ifb
heartbeat for science in society

**KATHOLIEKE UNIVERSITEIT
LEUVEN**

Overview

Social determinants linked to:

1. Information

2. Communication

3. People

1. Information

1. Information

The abstract view



I began to think of information as matter,



Page 113

7

THE MATHEMATICAL ROAD
TO THE FUTURE

1. Information

The embedded view



Dealing with information is not processing dead matter.
Information is dealt with/ “interpreted” in a lived context
including ... human bodies ... infrastructures ...
... ongoing practices...

1. Information

The embedded view



QUESTION. Can ICT-technology deal with “information”?

- Not really. Apart from simple things

1. Information

The embedded view



QUESTION. Can ICT-technology deal with “information”?

- Not really !!!!! As long as a computer does not become an embodied member of human society, sharing human ambitions and limits

1. Information

The embedded view

- **ARTIFICIAL INTELLIGENCE ?**



1972

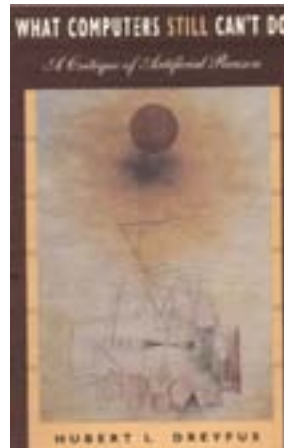


Hubert L. Dreyfus

■ **ARTIFICIAL INTELLIGENCE ?**



1972



1992



Hubert L. Dreyfus

2011

■ **SELECTING RELEVANT WEBSITES? GOOGLE?**



1999



Hubert L. Dreyfus

2011

■ **SELECTING RELEVANT WEBSITES? GOOGLE?**



1999



2009



Hubert L. Dreyfus

2011

Intelligent software and internet

- **does NOT proces information as dead matter**
- **links its information processing to human embodied and embedded assessment**

2. Communication

2. Communication

The abstract view



I began to think of information as matter, and started to examine how the availability of new information brings about change.



Page 113

7

THE MATHEMATICAL ROAD
TO THE FUTURE

2. Communication

The abstract view



I began to think of information as matter, and started to examine how
the availability of new information brings about
change. Let us imagine there is a pipeline that allows a flow
of material towards what provides for a state of justice.



Page 113

7

THE MATHEMATICAL ROAD
TO THE FUTURE

2. Communication

The embedded view

Information Shifting

Problematic meaning

Communicating information is not organizing flow.

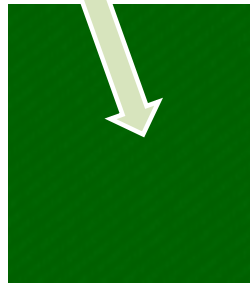
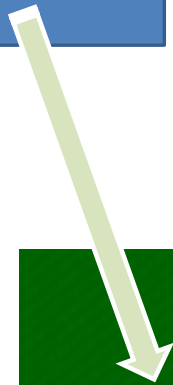
Communication is allowing other contexts to assimilate some of the meaning of the information

2. Communication

The embedded view

Information Shifting

Problematic meaning



2. Communication

The embedded view

Information Shifting

Problematic meaning



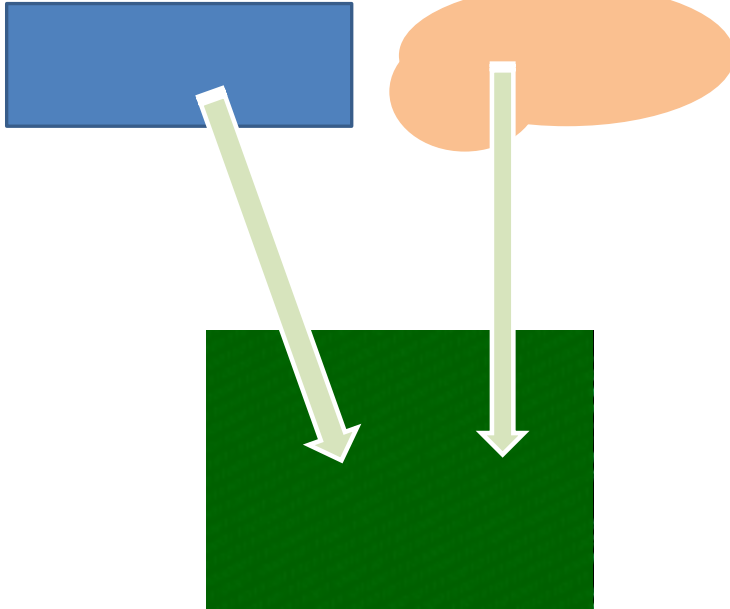
Thomas Hoepker, Williamsburg

2. Communication

The embedded view

Information Shifting

Problematic meaning

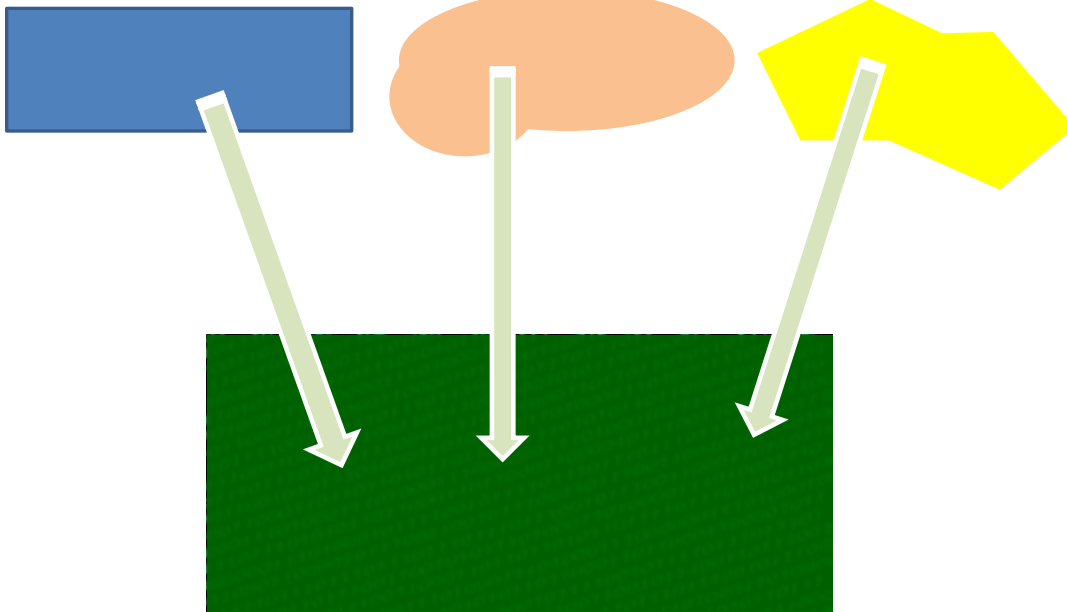


2. Communication

The embedded view

Information Shifting

Problematic meaning

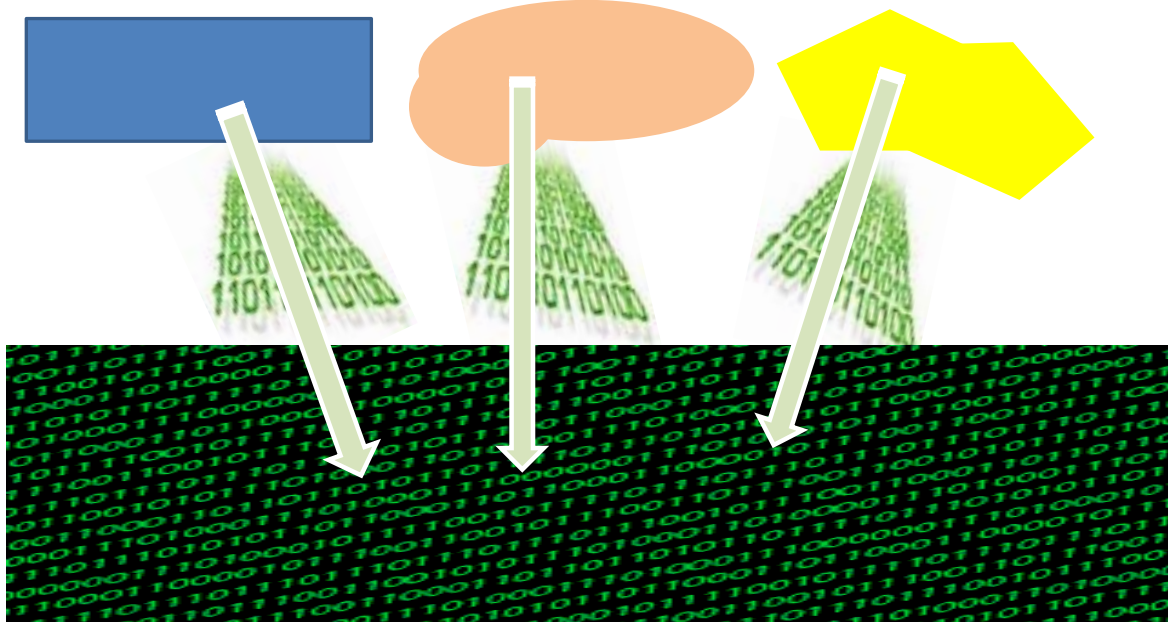


2. Communication

The embedded view

Information Shifting

Problematic meaning

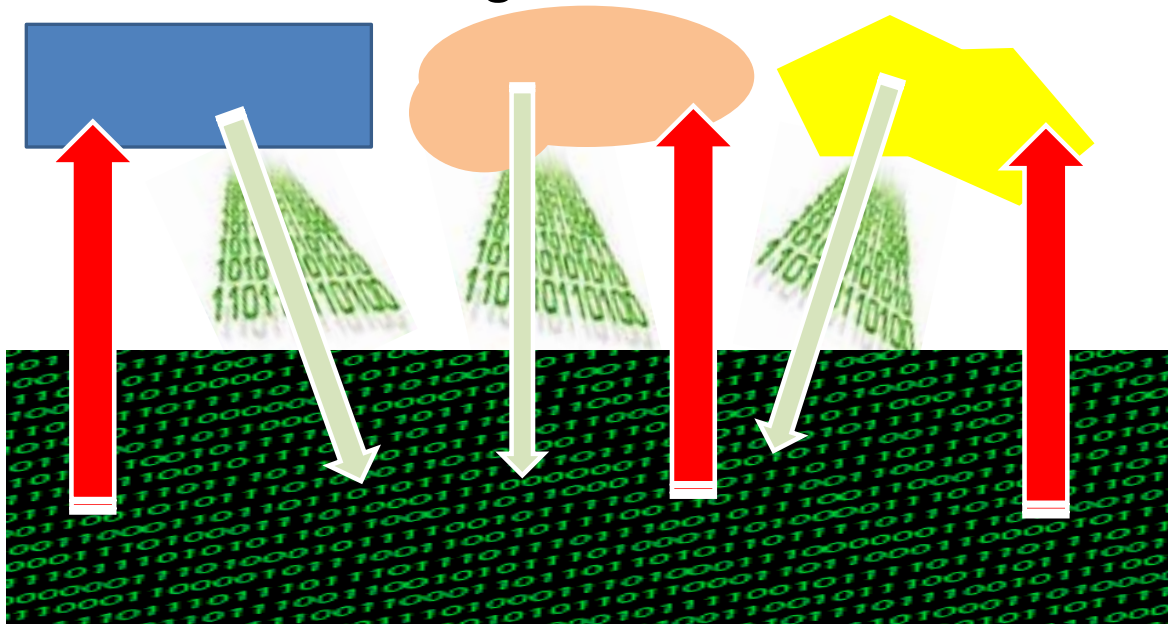


2. Communication

The embedded view

Information Shifting

Problematic action



Intelligent software and internet

- does NOT communicate information as dead matter
- is in permanent danger of
 - creating misunderstandings of information
 - triggering inappropriate action
- requires active translation
human assessment of
“context integrity” (>>
“privacy”)

3. People

3. People

The abstract view



I began to think of information as matter, and started to examine how it flows through people and through society, and how the availability of new information brings about change. Let us imagine there is a pipeline that allows a flow of material towards what provides for a state of justice.



Page 113

7

THE MATHEMATICAL ROAD
TO THE FUTURE

3. People

The embedded view

- Society is not a merely homogeneous or chaotic medium for information



3. People

The embedded view

Compare

The internet



World Wide Web



New communication technologies

3. People

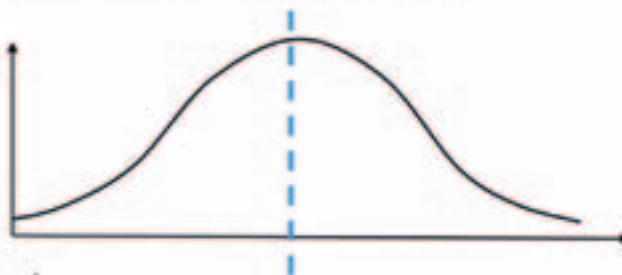
The embedded view



László Barabási

WWW reveals its topology

Centered around
an average scale



Scale free network

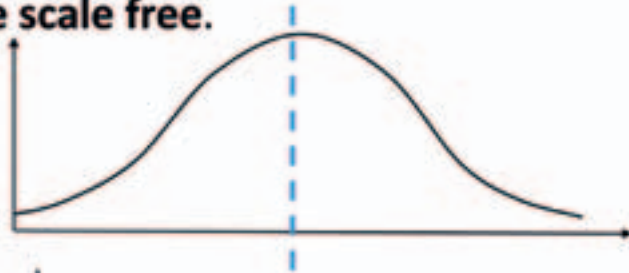




László Barabási

Many influential human networks are scale free.

Centered around an average scale



Scale free network



László Barabási

Many other structural elements of “random” society are now understood & integrated in operational models.

e.g. ■ The six degrees

■ The strength of “weak” ties

3. People

The embedded view



László Barabási

The dynamics of network structures is currently explored.

3. People

The embedded view



László Barabási

The dynamics of network structures is currently explored.

Preferential attachment

Richs get richer

How to break in?



3. People

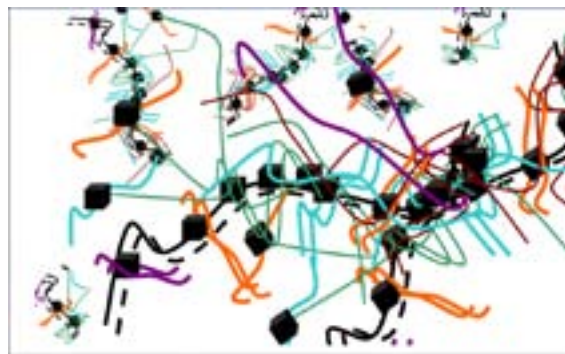
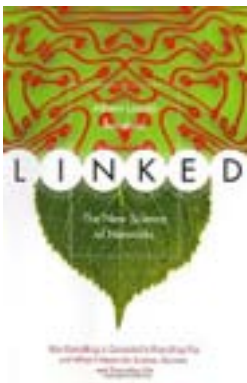
The embedded view



László Barabási

The dynamics of network structures is currently explored.

Total picture is complexity but not randomness and chaos



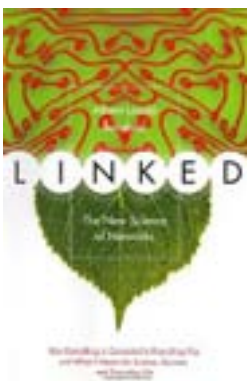
3. People

The embedded view



László Barabási

Network structures matter



3. People

The embedded view



László Barabási

Network structures matter

Importance for medicine,
innovation, ...

Importance for understanding
networks of people

Importance for understanding
possibilities of the www and the
inter-net



3. People

The embedded view



László Barabási

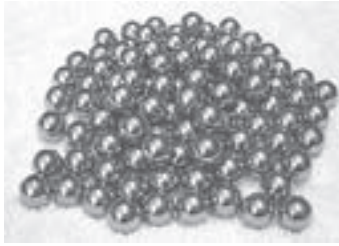
Network dynamics matter

Information is disseminated
in chains of action
and interpretation



Some key points

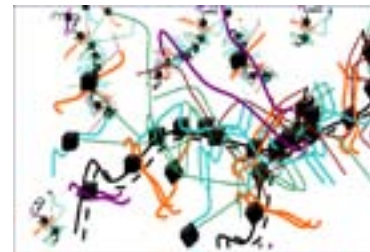
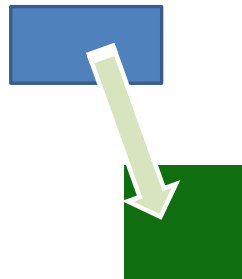
The embedded view



Information is
always embedded

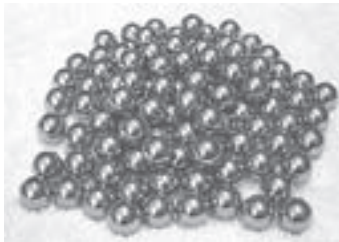
Communicating
is changing

ICT works for
networked people

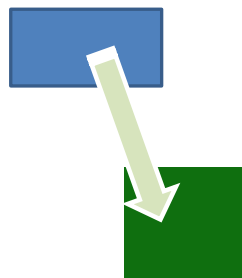


Some key points

The embedded view

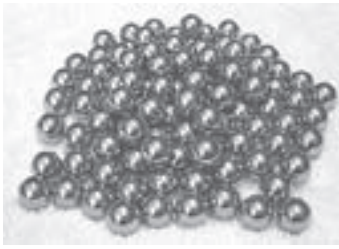


ICT is dealing with
embedded **Information & Communication** for embedded **people**



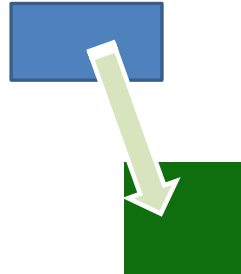
Some key points

The embedded view



ICT still too often assumes
it is dealing with dead matter in an amorphous society

ICT is dealing with
embedded **Information & Communication** for embedded **people**



Annex I

Participants



**Ethical aspects of information and
communication technologies**

Members of the European Group on Ethics (EGE)

Julian KINDERLERER
President

Professor of Intellectual Property Law, University of Cape Town, South Africa; Professor of Biotechnology and Society, University of Technology, Delft, the Netherlands

Linda NIELSEN

Vice-President
Professor of Global Law and Governance, doctor jurist, University of Copenhagen, Denmark

Paula MARTINHO da SILVA

Lawyer, visiting Professor and Senior Investigator at the Bioethics Institute, Portuguese Catholic University, Portugal

Emmanuel AGIUS

Professor of Moral Philosophy and Moral Theology, Faculty of Theology University of Malta, Malta

Inez de BEAUFORT

Professor of Health Care Ethics, Erasmus Medical Centre, Department of Medical Ethics Rotterdam, the Netherlands

Hille HAKER

Richard McCormick S. J. Chair of Catholic Moral Theology, Loyola University, Chicago, USA (since 2010); Professor of Moral Theology and Social Ethics, University of Frankfurt, Germany (since 2005)

Pere PUIGDOMÈNECH ROSELL

Research Professor of CSIC, Director of Plant Molecular Genetics Laboratory, CSIC-IRIA Barcelona, Spain

Günter VIRT

Professor emeritus of Moral Theology, University of Vienna, Austria

Peter DABROCK

Chair of Systematic Theology (Ethics), University of Erlangen-Nuremberg, Germany

Andrzej GORSKI

Professor of Medicine, Medical University of Warsaw and Polish Academy of Sciences, Poland

Ritva HALILA

Head of Department, Hjelt Institute, University of Helsinki (2010–13) leave of absence; General Secretary, National Advisory Board on Social Welfare and Health Care Ethics (ETENE), Finland

Herman NYS

Lawyer, Professor of Medical Law, Faculties of Law and Medicine, KU Leuven, Belgium

Siobhán O'SULLIVAN

Chief Bioethics Officer, Department for Health and Children, Lecturer in Healthcare Ethics and Law, Royal College of Surgeons of Ireland

Laura PALAZZANI

Full Professor of Philosophy of Law in Lumsa University, Rome, Italy

Marie-Jo THIEL

Professor, University of Strasbourg; Director of the European Centre for the Study and Teaching of Ethics (CEERE), University of Strasbourg, France

Secretariat of the EGE

Maurizio SALVI

European Commission
BEPA
Head of the EGE Secretariat

Kim-Hoang LÊ

European Commission
BEPA

Lauren O'CONNOR

European Commission
BEPA

Adriana-Sorina OLTEAN

European Commission
BEPA

Speakers

Fabrizio SESTINI

European Commission
Directorate-General for the Information Society and Media

Chengetai MASANGO

Programme and Technology Manager, United Nations Internet Governance Forum Switzerland

Dixie HAWTIN

Research and Policy
Global Partners and Associates
United Kingdom

William ECHIKSON

External Relations, Communications and Public Affairs, Head of Free Expression EMEA at Google
Belgium

Peter HUSTINX

European Union
European Data Protection Supervisor
(the European guardian of personal data protection)
Belgium

Lee HIBBARD

Council of Europe's coordinator on the information society and Internet governance
France

Michele BELLAVITE

ETNO — Chairman of the Digital Society Working Group
Belgium

Bernd CARSTEN-STAHN

De Montfort University
Professor of Critical Research in Technology and Director of the Centre for Computing and Social Responsibility
United Kingdom

Guido VAN STEENDAM

Professor of the Philosophy of Technology, KU Leuven; Director, International Forum for Biophilosophy
Belgium

National instances

Pete MILLS

Nuffield Council on Bioethics
United Kingdom

Wenceslaus Leonard KILAMA

Pan African Bioethics Initiative (PABIN)
Tanzania

Martina WEITSCH

Quaker Council for European Affairs
Belgium

Louise GUNNING-SCHEPERS
Heath Council of the Netherlands
The Netherlands

Constantin ZORBAS
Representation of Greece
to the European Union
Belgium

Gabriela BODEA
TNO — The Netherlands
Institute for Applied
Scientific Research
The Netherlands

Sonia ZDOROVITZOFF
European Juvenile Observatory
Belgium

Heidi HAVRANEK
Permanent Representation
of Austria
Belgium

Octávia FROTA
Belgium

Quirine A. M. EIJKMAN
International Centre for Counter-
Terrorism (ICCT)
The Hague

Joe McNAMEE
European Digital Rights
Belgium

Christopher HAYES
US Mission to the European Union
Belgium

Christian BORGGREEN
US Mission to the
European Union
Belgium

Representatives of religion, churches and communities of conviction

Kostas ZORMPAS
Theologian sociologist
Belgium

Stefanie HEUER
Evangelische Kirche
in Deutschland (EKD)
Belgium

Joseph P. DIMITROV
Continental Theological
Seminary
Belgium

Academics

Ugo PAGALLO
University of Turin
Italy

Luiz COSTA
Facultés universitaires Notre-Dame
de la Paix (FUNDP)
Belgium

Emily LAIDLAW
University of East Anglia Law School
United Kingdom

Salim MOKADDEM
University of Sciences and Technics
of Languedoc-Roussillon,
University Montpellier 2
France

Mireille HILDEBRANDT
Vrije Universiteit Brussels
Radboud Universiteit Nijmegen
Erasmus Universiteit Rotterdam
The Netherlands

John DOMINGUE
The Open University
United Kingdom

Marie des Neiges RUFFO
Université Paris-Sorbonne et
Facultés Universitaires Notre-Dame
De la Paix (FUNDP)
France

Christian DETWEILER
Delft University of Technology
The Netherlands

NGOs, agencies and associations

Caroline GANS COMBE
Reihoo
Versailles Saint Quentin en Yvelines
University
France/Switzerland

Contance BOMMELAER
The Internet Society
Switzerland

Innocenzo GENNA
AIP — Italian ISP Association
Belgium

Martin SCHMALZRIED
Coface (Confederation of Family
Organisations in
the EU)
Belgium

André BEECKMANS DE
WEST-MEERBEECK
Retired from the Belgian Nuclear
Research Centre
Belgium

Irma VAN DER PLOEG
Infonomics and New Media Research
Centre,
Zuyd University
Maastricht, the Netherlands

David WEBBER
PA Europe
Strategy Consulting and
Public Affairs
Belgium

Charles de MARCILLY
Fondation Robert Schuman
Belgium

Jörg JANSSEN
European Movement International
Belgium

Michael ROGERS
Belgium

Amélie COULET
APCO Worldwide
Belgium

Representatives of industry

Patricia WRUUCK
Google representative
Belgium

Cesare Marco PANCINI
Google representative
Belgium

Frederick DE BACKER
Telefonica SA
Belgium

Gilles DOWEK
INRIA Inventeurs du monde
numérique
France

Jarka CHLOUPKOVA
Profi press
Belgium

European Parliament

Fabrizio PORRINO
European Parliament
Information Society
and ICT Policies

Elina KAARTINEN
European Parliament
Committee on Industry,
Research and Energy (ITRE)

Bendert Zevenbergen
European Parliament

**BEPA (Bureau of European
Policy Advisers)**

Jan-David BLAESE
European Commission

**Research and
Innovation DG**

Giuseppe Giovanni DAQUINO
European Commission
Research Executive Agency to
the European Commission

Yves DUMONT
European Commission
Research and Innovation DG

Enterprise and Industry DG

Gordon BUHAGIAR
European Commission

**Information Society
and Media DG**

Nicole DEWANDRE
European Commission

Nicole ZWAANEVELD
European Commission

Loris PENSERINI
European Commission

Interpretation DG

Claude REPUSSARD
European Commission

Gaye COZORT
European Commission

Colin KOTZ
European Commission

Maren RAUSSER
European Commission

Jean-Marc PFAU
European Commission

Astrid EISENHAEUER
European Commission

Communication DG

Jennifer JACQUEMART
European Commission

Etienne ANSOTTE
European Commission

Annex II

Secretariat of the European Group on Ethics



Ethical aspects of information and
communication technologies

Secretariat of the European Group on Ethics



Maurizio SALVI,
MBA, MBS, PhD, D. Biotech.
European Commission
Head of the BEPA Ethics sector,
Head of the EGE Secretariat,

Berl 8/359, 1049 Brussels
E-mail: Maurizio.Salvi@ec.europa.eu



Kim Hoang LÊ
European Commission
EGE Secretariat

Berl 8/362, 1049 Brussels
Tel. +32 2299-9228
E-mail: Kim-Hoang.LE@ec.europa.eu



Adriana-Sorina OLTEAN
European Commission
EGE Secretariat

Berl 8/362, 1049 Brussels
Tel. +32 2299-3016
E-mail: Adriana-Sorina.Oltean@ec.europa.eu

Mail address

European Commission

Secretariat of the European Group on Ethics in Science
and New Technologies

Berlaymont Building
BERL 8/362
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

Office

European Commission
Berlaymont Building
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

Website

http://ec.europa.eu/european_group_ethics/index_en.htm

European Commission

Ethical aspects of information and communication technologies — Proceedings of the round-table debate

Luxembourg: Publications Office of the European Union

2012 — 173 pp. — 21 × 29.7 cm

ISBN 978-92-79-22327-3

doi:10.2796/13497

