



EUROPEAN PARLIAMENT

2009 - 2010

TEXTS ADOPTED

at the sitting of

Thursday
26 March 2009



P6_TA-PROV(2009)03-26

PROVISIONAL EDITION

PE 422.708

EN

United in diversity

EN

Strengthening security and fundamental freedoms on the Internet

European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI))

The European Parliament,

- having regard to the proposal for a recommendation to the Council by Stavros Lambrinidis on behalf of the PSE Group on strengthening security and fundamental freedoms on the Internet (B6-0302/2008),
- having regard to the International Covenant on Civil and Political Rights, the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the Charter of Fundamental Rights of the European Union, and in particular the provisions thereof relating to the protection of personal data, freedom of expression, respect for private and family life, as well as the right to liberty and security,
- 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 data,¹ to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,² to Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information,³ to the Commission's proposal of 13 November 2007 for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, 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 consumer protection cooperation (COM(2007)0698), to 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 networks⁴ and to the judgment of the Court of Justice of the European Communities of 10 February 2009 in Case C-301/06 *Ireland v Parliament and Council*,
- having regard to Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems,⁵ to Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment,⁶ to Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism,⁷ to the Commission's

¹ OJ L 281, 23.11.1995, p. 31.

² OJ L 350, 30.12.2008, p. 60.

³ OJ L 345, 31.12.2003, p. 90.

⁴ OJ L 105, 13.4.2006, p. 54.

⁵ OJ L 69, 16.3.2005, p. 67.

⁶ OJ L 149, 2.6.2001, p. 1.

⁷ OJ L 330, 9.12.2008, p. 21.

Communication of 22 May 2007 entitled ‘Towards a general policy and the fight against cyber crime’ (COM(2007)0267), as well as to the recent initiatives for the detection of serious crime and terrorism (such as the ‘Check the Web’ project),

- having regard to the work undertaken within the framework of the Council of Europe, the Organisation for Economic Co-operation and Development (OECD) and the United Nations (UN), both as concerns the combating of crime and cybercrime and as concerns the protection of fundamental rights and freedoms, including on the Internet¹,
 - having regard to the most recent judgments of the European courts and national constitutional courts in this field, and in particular the Judgment of the German Federal Constitutional Court recognising a distinct right to the protection of confidentiality and the integrity of information technology systems,²
 - having regard to Rule 114(3) and Rule 94 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Culture and Education (A6-0103/2009),
- A. whereas the evolution of the Internet proves that it is becoming an indispensable tool for promoting democratic initiatives, a new arena for political debate (for instance e-campaigning and e-voting), a key instrument at world level for exercising freedom of expression (for instance blogging) and for developing business activities, and a mechanism for promoting digital literacy and the dissemination of knowledge (e-learning); whereas the Internet has also brought with it an increasing number of opportunities for people of all ages to communicate with people from different parts of the world, for example, and has thereby expanded the scope for people to familiarise themselves with other cultures and thus enhance their understanding of other people and cultures; whereas the Internet has also extended the diversity of news sources for individuals as they are now able to tap into the flow of news from different parts of the world,
- B. whereas governments and public interest organisations and institutions should provide a suitable regulatory framework and appropriate technical means to allow citizens actively and efficiently to take part in administrative processes through e-government applications,
- C. whereas the Internet gives full meaning to the definition of freedom of expression enshrined in Article 11 of the Charter of Fundamental Rights of the European Union, especially in terms of its 'regardless of frontiers' dimension,
- D. whereas transparency, respect for privacy and an environment of trust amongst I-stakeholders should be considered indispensable elements in order to build a sustainable security vision for the Internet,

¹ E.g. Council of Europe Convention on Cybercrime of 23 November 2001; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.

² BVerfG, 1 BvR 370/07, 27.2.2008.

- E. whereas on the Internet, freedom of expression and privacy can at the same time be both better enhanced and more exposed to intrusions and limitations by both private and public actors,
- F. whereas, through the freedom that it provides, the Internet has also been used as a platform for violent messages such as the ones intentionally inciting terrorist attacks, as well as for websites which can specifically incite hate-based criminal acts, and whereas cybercrime threats more broadly have increased worldwide and are endangering individuals (including children) and networks,
- G. whereas these crimes must be countered effectively and decisively, without altering the fundamental free and open nature of the Internet,
- H. whereas, in a democratic society, it is the citizens who are entitled to observe and to judge daily the actions and beliefs of their governments and of private companies that provide them with services; whereas technologically advanced surveillance techniques, sometimes coupled with the absence of adequate legal safeguards regarding the limits of their application, increasingly threaten this principle,
- I. whereas individuals have the right to express themselves freely on the Internet (for instance user-generated content, blogs and social networking) and whereas Internet search engines and service providers have made it considerably easier for people to obtain information about, for example, other individuals; whereas, however, there are situations in which individuals wish to delete information held in such databases; whereas, therefore, companies must be able to ensure that individuals can have person-related data deleted from databases;
- J. whereas technological leaps increasingly allow for the secret surveillance, virtually undetectable to the individual, of citizens' activities on the Internet; whereas the mere existence of surveillance technologies does not automatically justify their uses, but whereas the overriding interest of protecting citizens' fundamental rights should determine the limits and precise circumstances under which such technologies may be used by public authorities or companies; whereas combating Internet crime and the threats to an open democratic society which certain persons and organisations constitute when they use the Internet to damage citizens' rights must not mean that Member States assume the right to intercept and monitor all data traffic on the Internet which occurs on their territory, whether that applies to their own citizens or data traffic from abroad; whereas the combating of crime must be proportionate to the nature of the crime;
- K. whereas identity theft and fraud are an increasing problem that the authorities, individual citizens and companies are only beginning to recognise, leaving major security concerns in relation to the intensified use of the Internet for a wide range of purposes, including commerce and the exchange of confidential information,
- L. whereas it should be recalled that, when dealing with rights such as freedom of expression or respect for private life, limitations to the exercise of such rights may be imposed by public authorities if they are in accordance with the law, necessary, proportionate, and appropriate in a democratic society,

- M. whereas, on the Internet, there is a major power and knowledge divide between corporate and government entities on the one hand, and individual users on the other; whereas, therefore, a debate must be launched on necessary limitations to “consent,” both in terms of what companies and governments may ask a user to disclose and to what extent individuals should be required to cede their privacy and other fundamental rights in order to receive certain Internet services or other privileges,
- N. whereas due to its global, open, and participatory nature, the Internet enjoys freedom as a rule, but this does not preclude the need to reflect (at national and international levels, as well as in public and in private settings) upon how the fundamental freedoms of Internet users as well as their security are respected and protected,
- O. whereas the host of fundamental rights that are affected in the Internet world include, but are not limited to, respect for private life (including the right to permanently delete a personal digital footprint), data protection, freedom of expression, speech and association, freedom of the press, political expression and participation, non-discrimination, and education; whereas the content of such rights, including their field of application and their scope, the level of protection provided by such rights and the prohibitions on abuse of such rights should be governed by the rules on the protection of human and fundamental rights guaranteed by the Constitutions of the Member States, international human rights treaties, including the ECHR, general principles of Community law and the Charter of Fundamental Rights of the European Union, and/or by other relevant rules of national, international and Community law, in their respective fields of application,
- P. whereas all the actors involved and active on the Internet should assume their respective responsibilities and engage in fora where pressing and important issues relating to Internet activity are discussed in order to seek and promote common solutions,
- Q. whereas e-illiteracy will be the new illiteracy of the 21st Century; whereas ensuring that all citizens have access to the Internet is therefore equivalent to ensuring that all citizens have access to schooling, and whereas such access should not be punitively denied by governments or private companies; whereas such access should not be abused in pursuit of illegal activities; whereas it is important to deal with emerging issues such as network neutrality, interoperability, global reachability of all Internet nodes, and the use of open formats and standards,
- R. whereas the international, multicultural and especially multi-lingual character of the Internet is not yet fully supported by the technical infrastructure and protocols of the World Wide Web,
- S. whereas in the on-going process of the "Internet Bill of Rights," it is important to take into account all relevant research and undertakings in the field, including recent EU studies on the topic¹,

¹ A recent study on 'Strengthening Security and Fundamental Freedoms on the Internet – an EU Policy on the Fight Against Cyber Crime' puts forward among other ideas the adoption of a non-binding Internet Bill of Rights.

- T. whereas economic activity is important for the further dynamic development of the Internet, while the safeguarding of its economic efficiency should be ensured through fair competition and the protection of intellectual property rights, as necessary, proportionate and appropriate,
- U. whereas the right balance should be maintained between the re-use of public sector information which opens unprecedented opportunities for creative and cultural experimentation and exchange, and the protection of intellectual property rights,
- V. whereas throughout the world, companies in the information and communications technology (ICT) sector face increasing government pressure to comply with domestic laws and policies in ways that may conflict with the internationally recognised human rights of freedom of expression and privacy; whereas positive steps have been taken, among which that taken by a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics who have created a collaborative approach with the aim of protecting and advancing freedom of expression and privacy in the ICT sector, and have formed the Global Network Initiative (GNI)¹,
- W. whereas strong data protection rules are a major concern for the EU and its citizens, and Recital 2 of Directive 95/46/EC on data protection clearly states that technology (i.e. data-processing systems) is “designed to serve man” and must respect “fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals”,
1. Addresses the following recommendations to the Council:

Full and safe access to the Internet for all

- (a) participate in efforts to make the Internet an important tool for the empowerment of users, an environment which allows the evolution of ‘bottom up’ approaches and of e-democracy, while at the same time ensuring that significant safeguards are established as new forms of control and censorship can develop in this sphere; the freedom and protection of private life that users enjoy on the Internet should be real and not illusory;
- (b) recognise that the Internet can be an extraordinary opportunity to enhance active citizenship and that, in this respect, access to networks and contents is one of the key elements; recommend that this issue be further developed on the basis of the assumption that everyone has a right to participate in the information society and that institutions and stakeholders at all levels have a general responsibility to assist in this development, thus attacking the twin new challenges of e-illiteracy and democratic exclusion in the electronic age²;

¹ <http://www.globalnetworkinitiative.org/index.php>.

² In the document entitled ‘Internet – a critical resource for all’ of the Council of Europe of 17 September 2008 it is also stressed that ‘ensuring and promoting equity and participation with respect to Internet is an essential step for the progress of equity and participation in the society at large’.

- (c) urge Member States to respond to a growing information-aware society and to find ways of providing greater transparency in decision-making through increased access by their citizens to information stored by governments in order to allow citizens to take advantage of that information; apply the same principle to its own information;
- (d) ensure together with other relevant actors that security, freedom of expression and the protection of privacy, as well as openness on the Internet, are approached not as competing goals, but instead are delivered simultaneously within a comprehensive vision that responds adequately to all these imperatives;
- (e) ensure that the legal rights of minors to protection from harm, as prescribed by the UN Convention on the Rights of the Child and as reflected in EU law, are fully reflected in and across all relevant actions, instruments or decisions relating to strengthening security and freedom on the Internet;

Strong commitment to combating cybercrime

- (f) invite the Presidency of the Council and the Commission to reflect on and develop a comprehensive strategy to combat cybercrime, pursuant, inter alia, to the Council of Europe Convention on Cybercrime, including ways in which to address the issue of “identity theft” and fraud at EU level in cooperation with both Internet providers and user organisations, as well as the police authorities dealing with IT-related crime and to put forward a proposal on how to create awareness campaigns and prevent such crime, while at the same time ensuring that the use of the Internet is safe and free for all; call for the creation of an EU desk for assistance to victims of identity theft and identity fraud;
- (g) encourage reflection on the necessary cooperation between private-public players in this field and on the enhancement of law enforcement cooperation, along with appropriate training for law enforcement and judicial authorities, including training on issues of fundamental rights protection; recognise the need for shared responsibility and the benefits of co-regulation and self-regulation as efficient alternatives or complementary instruments to traditional legislation;
- (h) ensure that the work undertaken in the framework of the "Check the Web" project and the recent initiatives aimed at improving the circulation of information on cybercrime, including by the setting-up of national alert platforms and a European alert platform for reporting offences committed on the Internet (creation of a European platform for cybercrime by Europol) are necessary, proportionate and appropriate and accompanied by all the necessary safeguards;
- (i) urge Member States to update legislation to protect children using the Internet, in particular in order to criminalise grooming (online solicitation of children for sexual purposes), as defined in the Council of Europe Convention of 25 October 2007 on the Protection of Children against Sexual Exploitation and Sexual Abuse;

- (j) encourage programmes to protect children and educate their parents as set out in EU law with respect to the new e-dangers and provide an impact assessment of the effectiveness of existing programmes to date; in doing so, take particular account of the online games which primarily target children and young people;
- (k) encourage all EU computer manufacturers to pre-install child protection software that can be easily activated;
- (l) proceed to the adoption of the directive on criminal measures aimed at the enforcement of intellectual property rights, following an assessment, in the light of contemporary innovation research, of the extent to which it is necessary and proportionate, and while simultaneously prohibiting, in pursuit of that purpose, the systematic monitoring and surveillance of all users' activities on the Internet, and ensuring that the penalties are proportionate to the infringements committed; within this context, also respect the freedom of expression and association of individual users and combat the incentives for cyber-violations of intellectual property rights, including certain excessive access restrictions placed by intellectual property holders themselves;
- (m) ensure that the expression of controversial political beliefs through the Internet is not subject to criminal prosecution;
- (n) ensure that there are no laws or practices restricting or criminalising the right of journalists and the media to gather and distribute information for reporting purposes;

Constant attention to the absolute protection and enhanced promotion of fundamental freedoms on the Internet

- (o) consider that “digital identity” is increasingly becoming an integral part of our ‘self’ and in this respect deserves to be protected adequately and effectively from intrusions by both private and public actors – thus, the particular set of data that is organically linked to the “digital identity” of an individual should be defined and protected, and all its elements should be considered inalienable personal, non-economic and non-tradable rights; take due account of the importance of anonymity, pseudonymity and control of information flows for privacy and the fact that users should be provided with, and educated about, the means to protect it efficiently, for instance through various available Privacy-Enhancing Technologies (PETs);
- (p) ensure that Member States that intercept and monitor data traffic, regardless of whether that applies to their own citizens or to data traffic from abroad, do so under the strict conditions and safeguards provided for by law; call on Member States to ensure that remote searches, if provided for by national law, are conducted on the basis of a valid search warrant issued by the competent judicial authorities; note that simplified procedures for conducting remote searches in comparison with direct searches are unacceptable, as they infringe the rule of law and the right to privacy;

- (q) recognise the danger of certain forms of Internet surveillance and control aimed also at tracking every 'digital' step of an individual, with the aim of providing a profile of the user and of assigning 'scores'; make clear the fact that such techniques should always be assessed in terms of their necessity and their proportionality in the light of the objectives they aim to achieve; emphasise also the need for an enhanced awareness and informed consent of users with respect to their e-activities involving the sharing of personal data (for instance in the case of social networks);
- (r) urge the Member States to identify all entities which use Net Surveillance and to draw up publicly accessible annual reports on Net Surveillance ensuring legality, proportionality and transparency;
- (s) examine and prescribe limits to the 'consent' that can be requested of and extracted from users, whether by governments or by private companies, to relinquish part of their privacy, as there is a clear imbalance of negotiating power and of knowledge between individual users and such institutions;
- (t) strictly limit, define and regulate the cases in which a private Internet company may be required to disclose data to government authorities, and further ensure that the use of that data by governments is subject to the strictest data protection standards; establish effective control and evaluation of that process;
- (u) stress the importance of Internet users being able to enhance their right to obtain the permanent deletion of their personal data located on Internet websites or on any third party data storage medium; ensure that such a decision by users is respected by Internet service providers, e-commerce providers and information society services; ensure that Member States provide for the effective enforcement of citizens' right of access to their personal data, including, as appropriate, the erasure of such data or its removal from web sites;
- (v) condemn government-imposed censorship of the content that may be searched on Internet sites, especially when such restrictions can have a 'chilling effect' on political speech;
- (w) call on the Member States to ensure that freedom of expression is not subject to arbitrary restrictions from the public and/or private sphere and to avoid all legislative or administrative measures that could have a "chilling effect" on all aspects of freedom of speech;
- (x) recall that transfer of personal data to third countries must take place in accordance with the provisions laid down in, inter alia, Directive 95/46/EC and in Framework Decision 2008/977/JHA;
- (y) draw attention to the fact that the development of the 'Internet of things' and the use of Radio Frequency Identification (RFID) systems should not sidestep the protection of data and of citizens' rights;
- (z) call on the Member States to apply Directive 95/46/EC on personal data in relation to the Internet correctly; remind the Member States that this Directive,

especially Article 8, applies regardless of the technology used for the processing of personal data and that its provisions call for Member States to provide the right to a judicial remedy and compensation for their infringement (Articles 22, 23, and 24);

- (aa) encourage the incorporation of fundamental principles of the “Internet Bill of Rights” into the research and development process of Internet-related instruments and applications and the promotion of the “privacy by design” principle according to which privacy and data protection requirements should be introduced as soon as possible in the life cycle of new technological developments, assuring citizens a user-friendly environment;
- (ab) support and request the active involvement of the European Data Protection Supervisor and of the Article 29 Working Party in the development of European legislation dealing with Internet activities with a potential impact on data protection;

International undertakings

- (ac) exhort all Internet players to engage in the on-going process of the “Internet Bill of Rights,” which builds on existing fundamental rights, promotes their enforcement, and fosters the recognition of emerging principles; in this respect the dynamic coalition on the Internet Bill of Rights has a leading role to play;
- (ad) ensure that, in this context, a multi-stakeholder, multi-level, process-oriented initiative and a mix between global and local initiatives are considered in order to specify and protect the rights of Internet users and thereby ensure the legitimacy, accountability and acceptance of the process;
- (ae) recognise that the global and open nature of the Internet requires global standards for data protection, security and freedom of speech; in this context call on Member States and the Commission to take the initiative for the drawing up of such standards; welcome the resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection of the 30th International Conference of Data Protection and Privacy Commissioners held in Strasbourg, on 15–17 October 2008; urge all EU stakeholders (public as well as private) to engage in this reflection;
- (af) stress the importance of developing a real Web E-agora where Union citizens can have a more interactive discussion with policy makers and other institutional stakeholders;
- (ag) encourage the active participation of the EU in different international fora dealing with global and localised aspects of the Internet, such as the Internet Governance Forum (IGF);
- (ah) take part together with all the relevant EU actors in the establishment of a European IGF that would take stock of the experience gained by national IGFs,

function as a regional pole, and relay more efficiently Europe-wide issues, positions and concerns in the upcoming international IGFs;

o

o o

2. Instructs its President to forward this recommendation to the Council and, for information, to the Commission.