

EUROPEAN PARLIAMENT

2004



2009

Committee on Civil Liberties, Justice and Home Affairs

2008/2160(INI)

21.1.2009

DRAFT REPORT

with a proposal for a European Parliament recommendation to the Council on
strengthening security and fundamental freedoms on the Internet
(2008/2160(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Stavros Lambrinidis

CONTENTS

	Page
PROPOSAL FOR A EUROPEAN PARLIAMENT RECOMMENDATION TO THE COUNCIL.....	3
PROPOSAL FOR A RECOMMENDATION TO THE COUNCIL (B6-0302/2008)	9
EXPLANATORY STATEMENT	11

PROPOSAL FOR A EUROPEAN PARLIAMENT RECOMMENDATION 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,¹ 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,² 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,³ 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,⁴ 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 networks⁵ and the Advocate General's Opinion of 14 October 2008 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,⁶ to Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment,⁷ to Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework

¹ OJ C 364, 18.12.2000, p. 1.

² OJ L 281, 23.11.1995, p. 31.

³ OJ L 350, 30.12.2008, p. 60.

⁴ OJ L 345, 31.12.2003, p. 90.

⁵ OJ 2006 L 105, p. 54.

⁶ OJ L 69, 16.3.2005, p. 67.

⁷ OJ L 149, 2.6.2001, p. 1.

Decision 2002/475/JHA on combating terrorism,¹ to the Commission's 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 (CoE), 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 Internet,²
 - 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,³
 - 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 (A6-0000/2008)],
- A. whereas the evolution of the Internet proves that it is becoming an indispensable tool for promoting democratic initiatives, a new arena for the political debate (e.g., e-campaigning, e-voting), a key instrument at world level for exercising freedom of expression (e.g., blogging) and for developing business activities,
- B. 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 its 'regardless of frontiers' dimension,
- C. 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 on the Internet,
- D. whereas, through the freedom that it provides, the Internet has also been used as a platform for violent and undemocratic messages such as the ones inciting to terrorist attacks, and whereas cybercrime threats more broadly have increased worldwide and are endangering individuals (including children) and networks,
- E. whereas these crimes must be countered effectively and decisively, without altering the fundamental free and open nature of the Internet,
- F. 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, and not the governments or companies who are entitled to

¹ OJ L 330, 9.12.2008, p. 21.

² Ex.: 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.

³ BVerfG, 1 BvR 370/07, 27.2.2008, Absatz-Nr. (1 - 333).

observe and to judge daily the actions and beliefs of their citizens; whereas technologically advanced surveillance techniques, combined with lax laws prescribing the limits of their application, increasingly threaten this principle,

- G. whereas technological leaps increasingly allow for the secret and virtually undetected surveillance of citizens' activities on the Internet; whereas the mere existence of surveillance technologies should 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 private companies,
 - H. whereas it should be recalled that, when dealing with rights such as freedom of expression or respect for private life, interferences with the exercise of such rights may only be imposed by public authorities if they are 'in accordance with the law' and necessary and proportionate in a democratic society,
 - I. 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, in public and in private settings) on how the fundamental freedoms of Internet users as well as their security are respected and protected,
 - J. 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 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,
 - K. 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,
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,¹ thus attacking the twin new challenges of e-illiteracy and democratic exclusion in the electronic age;²

- (c) ensure together with other relevant actors that security, freedom of expression and 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;

Strong commitment to combating cybercrime

- (d) invite the Presidency of the Council and the Commission to reflect on a comprehensive strategy in order to combat cybercrime, including the ways in which to address the issue of “identity theft” at EU level;
- (e) encourage reflection on the necessary cooperation between private-public players in this field and on the enhancement of law enforcement cooperation;
- (f) pursue the work undertaken within the framework of the Check the Web project and promote actions aiming at improving the circulation of information on cybercrime, such as the recent initiatives for setting up national alert platforms and a European alert platform for reporting offences committed on the Internet, provided that the necessary safeguards are in place;
- (g) 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;
- (h) proceed to the adoption of the directive on criminal measures aimed at the enforcement of intellectual property rights 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;
- (i) ensure that the expression of controversial political beliefs through the Internet, including with regard to terrorism, is not subject to criminal prosecution;

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

- (j) 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

¹ See Greek Constitution and its paragraph 5A.

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

intrusions by both private and public actors; 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 the means to efficiently protect it;

- (k) recognise the danger of 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 (e.g., the case of social networks);
- (l) 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;
- (m) strictly limit and define the cases in which a private Internet company may be required to disclose data to government authorities;
- (n) 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;
- (o) 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 the speech of individuals;
- (p) draw attention to the fact that the development of the 'Internet of things' should not sidestep the protection of data and of citizens' rights;
- (q) encourage 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 lifecycle of new technological developments;

International undertakings

- (r) 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;
- (s) 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;
- (t) 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);

- (u) 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.

11.6.2008

PROPOSAL FOR A RECOMMENDATION TO THE COUNCIL (B6-0302/2008)

pursuant to Rule 114(1) of the Rules of Procedure

by Stavros Lambrinidis

on strengthening security and fundamental freedoms on the Internet

The European Parliament,

- having regard to the European Convention on Human Rights and the Charter of Fundamental Rights, and in particular the clauses thereof relating to the protection of personal data, freedom of expression and information and respect for private and family life,
 - having regard to the recent initiatives for the detection of serious crime and terrorism ('Check the Web' project) and the recent proposal to amend Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, as well as the proposal for a review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications,
 - having regard to the work undertaken in the Council of Europe (CoE), the Organisation for Economic Cooperation and Development (OECD) and the United Nations (UN), both as concerns combating crime and cyber-crime and as concerns the protection of fundamental rights and freedoms, including on the Internet,
 - 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,
 - having regard to Rule 114(1) of its Rules of Procedure,
- A. whereas the Internet has become a key instrument at world level for exercising freedom of expression and developing business activities; whereas these circumstances make it all the more crucial, in the course of combating crime and also abuses of public and private powers, not to limit the potential of that instrument,
- B. whereas the worldwide scope, rapid development and specific technical characteristics of the Internet make it difficult to supervise through national legislation alone, and initiatives should be taken, not least at international level, to protect the rights of individuals in terms of both their security and their freedoms and protection of their private lives,

1. Addresses the following recommendations to the Council:

- a) facilitate a gradual alignment in the EU of national legislation concerning the requirements relating to the protection of fundamental rights on the Internet,
 - b) take steps to intensify the dialogue between national and European legislators and between national and European courts,
 - c) promote the dialogue between all those involved in and affected by the Internet, and particularly Internet operators and users,
 - d) promote conclusion of the necessary international agreements, both at a bilateral (and notably Transatlantic) and at a multilateral level (CoE, OECD and UN initiatives);
2. Instructs its President to forward this recommendation to the Council and, for information, to the Commission.

EXPLANATORY STATEMENT

Fundamental Rights on the Internet – enhanced and endangered at the same time

We live in an age where everyone, from governments to police, private companies and even criminals, seek the greatest possible access to our private electronic data. The Internet in particular provides previously unimaginable details about our private lives; even a single click on a website generates data that potentially could be used or abused by marketers, intelligence services, or identity thieves.

Therefore, ensuring the protection of the **fundamental right to privacy** on the Internet is one of the most urgent tasks that we as legislators face. It is also one of the thorniest ethical, legal, technological, and political challenges our societies ever have confronted.

It is clear to everyone that the Internet can be a tool to expand our fundamental rights, empowering us with boundless information and connecting us with individuals and communities around the world. It is somewhat less well acknowledged that, in the process, the Internet also poses a profound danger to our fundamental rights, potentially exposing us to pernicious surveillance, while serving as a tool for criminals and even terrorists. And least clear of all is how we can regulate the Internet in such a way that allows us to draw on its benefits, while limiting the very real and serious dangers of abuse. This calculus is made all the more complicated by the inherent nature of the Internet — a decentralized, user-driven network that is under the control of no government and that transcends nearly all borders.

This report, therefore, aims to highlight how we can best protect and promote the fundamental freedoms of individuals in an online environment. Among the essential elements of our response should be to:

- Involve all stakeholders;
- Act at different levels, making use of existing national, regional, and international instruments and observing how they are applied in today's legislative practice;
- Exchange best practices; and
- Respond to the needs and problems of various types of Internet users and of many (and constantly evolving) kinds of online activities.

Striking an appropriate balance between privacy and security is at the heart of our mission. It will demand constant vigilance and recalibration, so that we stay in sync with technology's irrepressible march. We must carefully consider security concerns of all kinds, from questions of national security, to the security and reliability of our networks, to the personal security of individuals as they share their data online. If ensuring a safer Internet is a legitimate objective for our societies, then we must address and constrain the use of surveillance and monitoring techniques that might threaten our fundamental freedoms—especially when their necessity, proportionality, and efficiency are in question. Flexibility, adaptability, and accountability must be the hallmarks of any legislation and programs we develop, so that we are able to stay one step ahead of evolving technologies.

The Internet also can greatly enhance other fundamental rights, such as freedom of speech, of political action, and of association — but it just as easily can also undermine them. One recent instance of this debate was the legislative initiative for monitoring of speech on the Internet in order to prevent terrorist attacks. This is a classic example of legislation that, unless very narrowly tailored to achieve its goals, could open up the door to massive surveillance, thus "chilling" the political speech of individuals — which is at the heart of a democratic society.

Finding the right balance on points such as this is crucial. There is no question that the Internet has bestowed on criminals a powerful new set of tools, and it goes without saying that terrorists should be prevented from using the Internet to plan and execute attacks. Likewise, our societies rightly demand that we thwart child pornographers on the Internet. Such criminals, in posing tangible threats, lower resistance among our citizens to police calls for widespread monitoring of the Internet — which, by its nature, is "intangible". We must resist this tendency. Our laws must be effective in fighting crime, but they must not be excessive. The Internet, by its more amorphous and intangible nature, renders itself open to such excesses. For example, few people would accept the notion that the police or marketing companies might open up every letter sent via the post office to check its content. Similar vigilance is required when protecting the content of electronic communications.

But speech may be chilled and privacy invaded not only by government authorities in pursuit of criminals, but also by private Internet companies in pursuit of profit. The newest tendency when this transpires — and usually only after companies are caught red-handed collecting, storing, and using our data without authorization -- is to demand the "**consent**" of the user (either on an opt-in or an opt-out basis) for the use of his or her data.

We must ask ourselves, "**What are the limits of consent?**" This question applies both to what a company can ask a user to disclose, and to what an individual should be allowed to cede of his privacy and other fundamental rights in order to receive certain Internet services or privileges.

The answers to these questions are not so straightforward. In another domain — that of labor legislation — our societies have agreed that there are limits to citizens' consent over their private lives. Labor law and collective bargaining agreements in most member states determine, for example, maximum working hours, minimum wages, or other labor rights, which individuals cannot be asked to "negotiate away" with their employers. The reason is simple: It is presumed that there is no balance of power between employee and employer and that, consequently, "consent" cannot be fairly given or extracted on an equal basis. Another reason is that we have also decided that we must prevent a "race to the bottom" upon the whole body of labor rights, which could ensue if some individual workers were allowed or "forced" to negotiate away some of their rights.

A similar power and knowledge gap exists on the Internet: Corporate and government power, knowledge, and interests prevail mightily over the individual user, as does the danger of offering "cheaper" (and thus more "attractive" for some users) Internet services in exchange for lower privacy protections. It is this Rapporteur's conviction that the next battle in the Internet security and privacy debate will be about the limits of "consent" sought by governments and private companies.

This issue must matter deeply to us because, in today's Europe, "Big Brother" will not come in the form of some authoritarian regime; it will come, if it does, stealthily and with our "consent".

Finally, **the right to Education and right of access to the Internet** are two additional rights that must be promoted in their own right, but which also could be threatened in the context of combating crime over the Internet. E-illiteracy will be the new illiteracy of the 21st century. As every child today has a right to schooling, and every adult to continuing education, every individual throughout their lifetimes should have the right to access computers and the Internet. Governments should ensure such access to even their remotest regions and poorest citizens; furthermore, it must not be denied as "punishment" for citizens' infractions. People from all walks of life, and from every region and culture, should be able to take advantage of the wide variety of services offered by the Internet. In this way, they can pursue their personal development, engage in educational, professional, and personal relationships, and foster economic opportunities to the fullest extent allowed by our technologies and our laws.