Telecom Package warning document for IMCO/ITRE vote, 07/07/08

Version 1.2 – First Release : June, 30th 2008 – Last modified : July, 2nd 2008

La Quadrature du Net has serious concern regarding several amendments that may be about to be adopted in the European Parliament in respect of the proposed Telecom Package in Parliament currently undergoing first reading. We believe these amendments seriously threaten the open architecture of the Internet, mere conduit principle and the rights and fundamental freedoms of its users.

The amendments are currently being negotiated in two European Parliament committees: Internal Market (IMCO) and Industry, Research and Energy (ITRE). If passed these harmful amendments agreed will be included in new draft law on the telecoms framework and consumer rights in respect of telecoms services. The Telecom Framework is what sets the rules for telecom operators and internet service providers across the EU's single market.

MEPs/ Press : for more information, Christophe Espern, +33 698 174 599

Summary

Amendment H1, proposed by the British Conservative MEP Malcolm Harbour, gives the European Commission the power to give recommendations about restrictions on "lawful content" access and distribution, or on execution of "lawful applications or services".

The Commission could, if this amendment is adopted, impose technical standards on content filtering and monitoring computing - so called "trusted computing". The Commission would be able to give the concerned by this regulation recommendations following a quick and undemocratic procedure, at the request of any national regulation authority (ARCEP, CSA, HADOPI in France, OFCOM in the UK, PTS in Sweden).

This amendment by Malcolm Harbour is supplemented by several further harmful amendments of fellow English Conservative MEP Syed Kamall, already adopted in the LIBE Committee, and which Mr. Harbour has announced he wanted to support.

Amendment K1 empowers the Commission to authorize "technical measures" to prevent or stop infringements of intellectual property. For this to occur it would be necessary to monitor and filter users' electronic communications with hardware and software, which in practice amounts to spyware replacing a judge and proper judicial oversight.

Amendment K2 authorises the automatic processing of traffic data without the consent of the user, if this treatment is practiced to ensure "the safety of a public service of electronic communication, a public or private electronic communications , a service of the information society and electronic communicating equipment. "

Amendment K2 is a major breach for the protection of personal data and privacy, as it allows businesses to remotely control user's electronic communications without their consent. Coupled with amendments H1 and K2 , it paves the way for the deployment of intrusive technologies on the client or in ISP boxes according to the whim of the Commission, and, also, the monitoring by the publishers of services and intermediaries (ISP and hosting), in the name of security and IPR.

In addition, two other amendments, H2 and H3, allow national regulatory authorities to impose access providers to work with rightsholders, in monitoring users specifically when their access is not "safe" (e.g. used to download), and to promote surveillance technologies mentioned above, which is similarly contained in the French draft law for graduated response.

This set of amendments creates in European law the unprecedented mechanism known as graduated response: Judicial authority and law courts are vacated in favour of private actors and "technical measures" of surveillance and filtering. According to rules set by administrative authorities and rights holders, intermediaries will be forced to cooperate in monitoring and filtering their subscribers, or exposed to administrative sanctions.

About La Quadrature du net (Squaring the net) – http://www.laquadrature.net

La Quadrature du Net / Squaring the Net is a european citizen group informing about legislative projects menacing civil liberties as well as economic and social development in the digital age.

La Quadrature du Net informs citizens, public authorities, organizations, corporations. It works with everyone to elaborate balanced alternative solutions.

La Quadrature du Net / Squaring the Net is supported by french, european and international NGOs including the Electronic Frontier Foundation, the Open Society Institute and Privacy International.

<u>Amendment H1, Harbour :</u> Allows national regulation authorities and the Commission to establish standards which restrict the run of « lawful applications » and « lawful services » and access and distribution of « lawful content » How a computer or an ISP can determine what is lawful and unlawful ? =>Paves the way to filtering and surveillance computing (known as « treacherous computing »).

A national regulatory authority may **issue guidelines setting** minimum quality of service requirements**, and, if appropriate, take other measures, in** order to prevent degradation of services and slowing of traffic over networks, **and to ensure that the ability of users to access or distribute lawful content or to run lawful applications and services of their choice is not unreasonably restricted. Those guidelines or measures shall take due account of any standards issued under article 17 of Directive 2002/121EC (Framework directive).**

The Commission may having examined such guidelines or measures and consulted [XXX], adopt technical implementing measures in that regards if it considers that the guidelines or measures may create barrier to the internal market. Theses measures designed to amend non-essential elements of this directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutinity referred to in article 37(2).

NB : 1) Treacherous computing is an expression used to avoid the use of Trusted Computing because so called technologies are designed to take off the right of users to control their computer (and by the way their personal data). One goal for producers is to be able to remotely control the use of their content as they do not trust users.

2) Free Software is not compatible with standards used to try to restrict the run of a « lawful application » : Free Software can be studied and modified by the user himself to check the security of the software or to create a new lawful application as Free Soffware authors grant the right to do so to every user. So beside pushing dangerous technologies for privacy, this amendment mays create by itself a barrier in the internal market even if an ISO standard of treacherous computing emerges like the following (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50970).

3) Please study this amendment from a strategic point of view and follow the reference to article 37(2) to understand why it is also a trojan horse from democratic point of view.

<u>Amendment K1, Kamal,</u> treacherous computing, opens the door to mandatory DRM/TPM, when linked with H1 and K2

Article 2 - point 5 a (new)
Directive 2002/58/EC
Article 14 - paragraph 1
(5a) In Article 14, paragraph 1 shall be replaced by the following:

1. **In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features*, including,*** *without limitation, for the purpose of detecting,intercepting or preventing infringement of intellectual property rights by users*, **are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.**

For information paragraph 2 and 3 mentionned in this paragraph 1 :

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(9).

3. 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(10).

NB : *this amendment opens the door to implementation of intrusive technologies that could become mandatory as far as these technologies do not impair internal market. First, this amendment states that it is possible to use technical measures to detect, intercept or prevent infringements of intellectual property rights (including infringements to copyright, trademarks right, and patents right). Yet, to detect, intercept and prevent such infringements, users' uses and electronic communications must be monitored with hardwares and softwares that are actually finks taking the place of police and judge (who usually is the only one who can tell what is lawful and what is not).*

Second, this amendment doesn't prevent from creating mandatory measures, as the only provision is that such requirements don't harm freedom to market and

competitiveness inside the Internal Market. Finally, reference to paragraph 3, which is by itself insufficient to protect privacy, is totally voided by the next amendment (Amendment K2 below).

Amendment K2, Kamal, treacherous computing, allows corporations to remotely control users' communications without their consent

Article 2 - point 4 a (new)
Directive 2002/58/EC
Article 6 - paragraph 6a (new)
(4a) In Article 6 the following paragraph 6a is added:

6a. Traffic data may be processed by any natural or legal person for the purpose of implementing technical measures to ensure the security of a public electronic communication service, a public or private electronic communications network, an information society service, or related terminal and electronic communication equipment. Such processing must be restricted to what is strictly necessary for the purposes of such security activity.

NB : the concept of security is used by DRMS (Digital Restriction Management System) vendors and also in national laws implementing the directive 2001/29EC which forbid the circumvention of technical measures used to control copy of works (as DRM try to). The directive itself states « the protection of technological measures should ensure a secure environment for the provision of interactive on-demand services ». So when reading this amendment, the security of an electronic communication equipment may be unterstand as the security of DRM preventing, detecting, or intercepting IP infringements (in compliance with amendments H1 and K1).

Amendement H2, Harbour : known part of french flexible response model, introduces the concept of cooperation between ISP and producers under the control of national regulation authorities, written by the french cinema lobby, SACD, works along with amendements H2, H3.

Article 33 (2a) – new

Without prejudice to national rules in conformity with community law promoting cultural and media policy objectives, such as cultural and linguistic diversity and media pluralism, national regulatory authorities and other relevant authorities shall also as far as appropriate promote cooperation between undertakings providing electronic communications networks and/or services and the sectors interested in the protection and promotion of lawful content in

electronic communication networks and services. These co-operation mechanisms may also include coordination of the public interest information to be made available as set out in Article 21(4a) and Article 20(2).

NB : La Quadrature du Net has evidences that this amendment was written by SACD
See : http://www.laquadrature.net/en/privacy-film-industry-pirates-european-law

Amendement H3, Harbour, known part of french flexible response, organizes blackmail by email and plans that costs for ISPs are at the charge of member states, same mechanism as in the french draft law on flexible response

Article 21 (4a) - new

Members state shall ensure that national regulatory authorities oblige the undertakings referred in paragraph 4 to distribute public interest information to existing and new subscribers when appropriate. Such information shall be produced by the relevant public authorities in a standardised format and may inter alia cover the following topics :

(a) illegal uses of electronic communications services, particularly where it may prejudice respect for the rights and freedoms of others, including infrigement of copyright and related rights ;

(b) the most common illegal uses of electronic communications services, including copyright infrigement, and their consequences; and

(c) means of protection against risks to personal security, privacy and personal data in using electronic communications services.

Significant additional costs incurred by an undertaking in complying with these obligations shall be reinbursed by the national regulatory authority.

NB : *this amendment forces Internet Access Providers (ISPs) to send notice messages to users when unlawful uses have been detected. The issue is that it doesn't tell who is the one asking to send the notice of illegal uses and who is detecting it (private actors, national regulatory authorities, judicial authority?)*

The difference between point (a) and point (b) should be noted: the first one aims at individual uses (informations on intercepted or detected allegedly infringements) whereas the second one is general (informations on most common cases of unlawful uses of Internet access).

Point (c) is about informations on traffic data processing means without permission for Internet access security reasons, authorized by Commission through amendment H1, K1, and K2. This is the exact description of informations that French government is eager to send to users in the so-called ***three-strikes approach*** *(graduated responses) in order that users install filtering and monitoring means.*