Note on the “flexible response” and the “telecom package”

François Pellegrini (pelegrin@labri.fr)

Version 1.0, 04/08/2008

Summary

Several amendments inserted on the “telecom package” have nothing to do with it. They have been written by members and sympathizers of the cultural contents industry, in order to track and control the circulation of numerical data, and to orient the behavior of Internet users towards using their content platforms through filtering and monitoring means, therefore violating the “network neutrality” paradigm.

The impact of these private interest amendments is dramatic: in addition to turning the worldwide public resource which Internet has become into a privatized distribution network for the benefit of a few players, they allow national regulation authorities to implement, without any democratic control, automated tools to monitor the behavior of Internet users, even from within their own computers (a practice sometimes advocated as “trusted computing”), and to ban them without any judicial decision from this worldwide resource (the so-called “graduated response” or “three-strikes” approach).

All of these sneaked amendments must be removed from the “telecom package”, to which they should not belong. Moreover, they pose in substance such a threat to the development of the information society that they should never be voted nor considered, but instead be rejected *en bloc*.

This note aims at explaining why.

The access revolution, abundance vs rarity

When cultural works were tied to their material support, such as printed books, vinyl records or even CDs, it was difficult for artists to reach their public. Therefore, players who were not artists themselves took in charge the role of duplicating and distributing the original works, acting as mediators between the artists and the public. Because of industrial concentration, and because not all edited works could be distributed, editors became in position to control the commercial success of artists, and eventually merged with producers so that production and edition decisions could be taken globally: either an artist would be produced and distributed so as to maximize return on investment, or else would not be produced at all. The concentration of these players maximized their revenue, but decreased cultural diversity as visible by the public, since only a limited number of artists could benefit from large scale advertising. Moreover, being in the situation of controlling distribution channels allowed them to set high prices which increased their profit even more[1].

The situation completely changed with the advent of the Internet. By allowing a direct contact between artists and their public at zero cost[2], the Internet makes possible to turn rarity into abundance: small music groups can find audiences very far from their region of origin by diffusing some of their works on personal or mutualized websites such as Myspace Music or Jamendo, and can sell and ship directly

1 It is reported that authors earn on average 7% of the retail price of a CD, that is, for a CD of 13 songs sold at 13 Euros, 7 cents of Euro per song,

2 While in the first days of the Internet users payed according to the volume of data transmitted, triple-play offers provide Internet and phone connectivity at a fixed, monthly price. Therefore, one can consider that the fee pays for his phone, and that Internet access is free irrespective of the amount of data transferred.

their records, with much higher benefits per copy than the ones they can get from traditional editors and distributors.
Any technological revolution favors some players and make others disappear. The access revolution makes editors useless, while the production function is still necessary, albeit with much lower costs through the generalization of audio and video processing software on home computers. Therefore, large editors have engaged in a way to slow down and even halt this process. It can only be done by reintroducing artificial rarity where abundance prevails; basically, it amount to finding ways to discriminate between types of contents and slowing down or filtering content not provided by major editor websites, such that users are inclined to buy their contents only from these latter.
The way that has been found is to define some content or actions as “unlawful” and, when such actions are considered “unlawful”, to deny users any right to proper service and absence of filtering. By reverting this logical proposition, it is clear that all of the sneaked amendments aim at legalizing content and protocol monitoring and filtering by denying “unlawful” users any right to complain about such measures.

How can you tell what is lawful and what is not ?

All of the amendments at stake create a distinction between “lawful” and “unlawful” matters. For instance, Compromise Amendment 5 on Article 22(3) deals with preserving “reasonably” (!) the quality of service of the Internet for “the access or distribut[ion of] lawful content” and the “run[ning of] lawful application and services”.
The key question is therefore: how can one know whether a content or an application is “lawful” or not? This is a critical issue, as the entity deciding on these matters has the power to shape the Internet at will, for instance excluding all innovative services which may endanger the interests backing this entity.
The answer, from a purely technical point of view, is: there is no way. Even a user sending a copyrighted audio file from one of his e-mail address to another may just be exercising its right to private copying, by transferring such files from his home computer to his business computer. It is only through human judgment that an action can be understood as licit or illicit.
However, the proponents of the amendments seem pretty sure that they can track down “unlawful content” and “unlawful applications and services”, the quality of service of which would not be guaranteed. How can they do that?
The only two ways for this are either to perform filtering *a priori* by discriminating against some technologies and communication protocols such as peer-to-peer systems without considering their use (as if all cars were banned because some can be used to break into shops) and therefore breaking Internet neutrality, or on the fly by spying on the contents of exchanged data, breaking laws on private correspondance.
Both are useless: encrypted communications prevent intermediate agents from analyzing the contents of exchanged data, and data transfer systems can be built on top of, for instance, e-mail systems, such that fragments of files can be sent when specific e-mail headers are used. The monitoring of these exchanges, all the more when performed by private entities, will necessarily frontally conflict with the right to private correspondance. Should this latter be surrogated to private interests?

The French graduated response is a no-go

Attempts to pave the way to some flavor of the French graduated response fail to consider an important point: it is unworkable both in principle and in practice, while harming civil liberties in a dramatic way.

This scheme was devised by the cultural content industry so as to replace long judicial procedures to

identify and prosecute music file sharers, by an automatic system to identify them, warn them and, after the third warning, ban them from the Internet for some period of time, without any possibility for them to register to another provider (basing on a black-list file). This scheme poses several strong legal problems which should prevent any pushing forward of the "telecom package" sneaked amendments.

- Regarding attributability, all of the warning and message sending measures base on what is called the "IP address" of the user's computer, as seen from the Internet, which is somewhat equivalent to the street number from which the data traffic originates and/or to which it is sent. The problem is that several members of the same family use the same address or even, for a company, that all of the traffic involving company computers are often seen as originating from the unique IP address of the company. Who will be prosecuted? Will a whole company be banned from the Internet? All of this is neglected and, as expected, leads to dramatic albeit funny results: in Finland, the first Internet user to be banned has been... the government of the autonomous territory of the Åland island! Too bad for the advance of e-administration...

  As it is extremely easy to break the security of any WEP-encrypted WiFi connection, one can even imagine actions of nuisance against prominent organizations and people to have them been targeted and banned from the Internet. As can be seen, by removing any requirement of burden of proof, legal uncertainty is increased for all Internet users.

  Shutting off the Internet access of a whole family if one of the member is considered[3] responsible of "unlawful" conduct is a disproportionate deprivation of freedom, as the Internet is now a way for people to get educated, to interact with administrations, to find jobs. It is as if, when someone is considered guilty of robbing an apple, all of his family had to stay locked in their home. Is it this, that Members of the European Parliament want in the digital age?

- The appeal procedure is designed not to be suspensive, because else the effect of the scheme would be marginal, since all defendants would appeal to court on the feebleness of the proof, creating the judicial bottlenecks the scheme wants to prevent. Consequently, in case of mistake, users can be prevented from accessing the Internet for several months, and be blacklisted, without any remedy, even if one's job depends on it.

- The sanctions planned in the graduated response framework cannot prevent right holders to launch civil and legal prosecutions. As the French Conseil Constitutionnel ruled during the voting of the DADVSI law (that is, the French transposition of the EUCD directive), in the field of copyright, either there is infringement and law cannot be prevented to apply, or there is not. The fact that some right holders may decline to sue Internet users when these are subject to automatic measures taken by national authorities is their own decision, which can be reconsidered at any time in the future, and may not be followed by other right holders. The massive tracking of Internet users is therefore not a compensation for the absence of lawsuits; these can still be launched when enough data has been massively collected.

- The role of monitoring user traffic is devoted to private entities which, in order to perform their task, must analyze the contents of the data exchanged, and therefore violate the right to private correspondance of the citizens using the Internet. This filtering will moreover be useless when citizens, to enforce this right, resort to encrypted communication channels. These encryption channels are already common, and recommended by many administrations to secure data exchanges against electronic interception by Echelon-like systems. I personally use them every time I connect to my computers. Will encrypted traffic be filtered out as being considered

3 It is deliberately that this word is used instead of "judged", as such actions are taken without any fair judgment.

"unlawful" by nature?

The action means envisioned by the graduated response framework are simply outdated and inefficient.

The legal aberration inherent to the graduated response scheme has been described in detail in the "Cédras" report[4], written by Jean Cédras, professor in law at the *Université de La Rochelle*. This report, ordered by the French Ministry of Culture, has been buried as soon as delivered because its conclusions did not match the short-term views of the major content providers.

The Swedish government also rejected this approach. Will the European Parliament endorse it by means of directives which have nothing to do with this issue?

The full story

During the last 15 years, in parallel to the spreading of the Internet, many proposed or adopted legislations have added new forms of sanctions to the ones already punishing infringement: legal prosecution against the circumvention of technical "protection"[5] measures (called "TPM" for short, since 1994 in the USA and then Europe), obligation to use some TPMs (SSSCAct in the USA and the so-called "Vivendi amendment" to the DADVSI law in France), ability of content providers to monitor network traffic (LCEN law in France in 2006), extreme preventive civil measures (directive 2004/48/CE, draft of the ACTA agreement), legal sanctions including for non-commercial infringement and incitement (draft of the IPRED2 directive and of the ACTA agreement), etc.
Most of these new forms of sanctions and fines are designed to be applied without any legal judgment, by creating automatic procedures which can take place even before any infringement happens. The graduated response scheme is part of this trend. As for all of the other measures, it has been the subject of world-wide lobbying (under the name of "three-strikes approach") by right holder lobbies, joined by the proponents of "trusted computing" devices such as the NGSCB[6] system (formerly known as "TCPA/Palladium") developed by Intel and Microsoft (which is a prominent member of the BSA lobby). This system did not meet commercial success, so any attempt to create such a market by law is welcome by these players.

Mandatory "security" measures threaten Europe's security

Compromise amendment 2 on Article 20 contains, in the second and last items of paragraph 2.b), puzzling mentions about the existence of "*restrictions imposed by the provider regarding a subscriber's ability to access, use or distribute lawful content or run lawful applications and services"*, and about "*any restrictions on the use of terminal equipment imposed by the provider*", of which the user should at least be informed. How come some user should be restricted in his ability to use the Internet, all the more if such actions are "lawful" ?

The answer resides in the will of content providers to restrict, on the user's own computer, his ability to use the cultural content he legally acquired. For instance, in 2004, SonyBMG added to some of its CDs a "technical protection measure" on the form of a software called XCP[7], which silently installed on the

4 `http://www.odebi.org/docs/RapportCedras.pdf` .

5 The double quotes are necessary because none of these measures effectively "protect" the works, which can still be copied digitally on their whole. They only secure the monopolies of content-reading software providers, tied to the editors which distribute content scrambled according to trivial but (originally) secret algorithms such as CSS.

6 `http://www.lebars.org/sec/tcpa-faq.html` .

7 `http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal` .

user's computer without any notice, and automatically prevented the user from undertaking such actions as copying audio files from the CD to other media. This software posed severe security threats, such as opening breaches that favored the installation of malicious software, but any attempts to remove it were legally impossible because it was assimilated to the circumvention of a TPM.

The purpose of NGSCB-like systems is much broader: it aims at preventing any “untrusted” program to access “premium content” locally stored on the user's computer or available through the Internet. On computers running these systems, any program which is not endorsed by the system maker cannot interact with this data. Here again, in this scheme, it is up to private entities to decide whether some new application which could offer a new and innovative service is able to access the user's own legitimate content, and therefore be of commercial interest to customers. In particular, libre/free software will never be considered, since for right holders the availability of the source code is a threat to the secrecy of the TPMs they implement (and which are anyway inefficient, being “broken” only a few months after they are released).

Being able to impose, through national authorities or so-called “stakeholders”, such “technical measures” is a subtle but most efficient way to bias the market against libre/free software and new services offered by innovative people or SMEs. Should users have specific vendor software to access the Internet? How can national and European security agencies assert that such software, secret by nature, does not contain backdoors[8] which would endanger Europe's informational independence?

In that respect, some dispositions of the “Alvaro report”, which pave the way to such behaviors, are to be taken very cautiously. For instance, Amendment 32 states: “*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*”. This amendment could be thought as preventing mandatory requirements on technical features; a careful reading shows on the opposite that, provided they do not “*impede the placing of equipment on the market*”, such mandatory technical requirements are completely allowed, all the more if they are provided by the very same vendor which also provides the computer software.

P2P is a tool, not a crime

The “P2P” term, shorthand for “Peer-to-peer”, refers to a technology for file sharing, software implementing this technology, and the numerous uses which are made of it.
Unlike traditional diffusion systems, in which a unique provider, called “server”, sends some information to all of the users' computers, called “clients”, the P2P technology is based on symmetry: all of the computers running the same P2P software can at the same time be clients, when the user wants to obtain on his local hard disk a full copy of a given file, but also be servers able to provide other users with parts of the files they want, if they are locally available.
Due to this feature, P2P software are a revolutionary tool for the creation and the diffusion of culture, as well as for the reduction of the digital divide.
Indeed, with a classical diffusion system, an author willing to diffuse the audio or video works he created should have an “upload” communication bandwidth (that is, the amount of data he can transfer from his computer to the Internet per unit of time) large enough to fulfill the requests of all of the

8 `http://www.heise.de/tp/r4/artikel/2/2898/1.html` .

Internet users willing to obtain his works from his website. Yet, ADSL-type technologies are not meant for that purpose: basing on the fact that users consume more information than they produce and distribute, the bandwidth of the ADSL link connecting a user computer to the Internet is ten times larger in the “descending” way (that is, going from the Internet to the user) than in the “ascending” way (the letter “A” of “ADSL” indeed meaning “asymmetric”, to acknowledge this asymmetry in communication capabilities).
Consequently, to broadcast his works, a creator should rent a communication channel of a much larger bandwidth, or rent some space on a professional server providing this amount of bandwidth.
P2P systems are the answer to this problem: as soon as several copies of the same file have already been downloaded by several users, when another user wishes to obtain this file, fragments of the file are sent to him by all of the users already having an (at least partial) copy of it. Therefore, the ascending bandwidths of these users are used concurrently to provide the new user with an amount of data equivalent to his descending bandwidth. Users benefit from a high-bandwidth access to the works, even when their creator has only a cheap ADSL access providing him a small ascending bandwidth.
Among the uses of the P2P technology, one can cite:

- the availability to all Internet users of the files representing the contents of CDs and DVDs of Linux software distributions,
- the P2PTelevision project, which aims at diffusing across the Internet audio-visual contents created by and for communities which have not usually access to conventional media (programs in regional tongues, for a local area, etc),
- the diffusion to Internet users, by its authors, of the *Starwreck* movie, the most ever seen Finnish movie,
- and many more examples.

P2P is therefore a revolutionary and extremely cheap technology for the creation of an inclusive information society. As any technology, it is neutral, and it is the uses which are made of it which can be legitimate or illegitimate. It is not because some use it to spread illegal content that this technology should be banned in itself.
One can however wonder who would be the main beneficiaries of a de facto forbidding of P2P technologies. Wouldn't it be the major content providers, which have means to own file servers with high ascending bandwidth, and which could see alternate diffusion networks as a threat to their rents?

Conclusion

The “telecom package” is a set of directive aiming at enforcing a free market on the telecommunication business sector, and at preserving the interest of consumers. It deals with the communication channels, and absolutely not with the contents and services which are offered and will be offered in the future.

Consequently, content-oriented amendments, which promote a specific rent model for some well-established players, and are likely to hinder the development of new services and players while harming Europe's informational independence, have nothing to do in them, all the more that they would be very hard to reconsider in the future.

All of these content-oriented amendments, which discriminate on an impossible basis between “lawful” and “unlawful” content, must be rejected *en bloc*. However, as the issue of the mutation of content services in the era of the Internet is critical, parliamentary debate is much welcome, in a framework that is still to be defined.