**ANALYSIS OF RECENT AMENDMENTS TO THE TELECOMS PACKAGE WITH PARTICULAR REFERENCE TO WARNINGS AND SANCTIONS RELATING TO ALLEGED UNLAWFUL USE OF COMMUNICATIONS NETWORKS – VERSION 4**

1. This work has been produced by Simon Bradshaw, as the Law in Practice element of his Bar Vocational Course, assisted by Professor Lilian Edwards, Professor of Internet Law at the University of Sheffield. As such the analysis herein does not constitute formal legal advice nor does it represent the views of the University of Sheffield.

2. We were asked to comment upon the proposed amendments to the key EU Directives governing telecommunications and related services, with particular reference to provisions that may permit summary disconnection of a user's Internet access in response to allegations of conduct such as infringement of copyright. Such measures have been referred to as 'graduated response' or 'three strikes'; in this analysis, we will refer to 'connection sanctions'. These amendments ('the Telecoms Package') were initially proposed by the EU Commission, and have been themselves amended further by the EU Parliament ('EUP'). We have helpfully been provided with the most recent version of some of the key element of the Telecoms Package as further amended by the Council of Ministers ('CoM'), and the EU Commission's latest revised version of the text. If the Commission can broker compromise between the CoM and EUP positions the Package may be passed before the end of the year. If compromise is not reached, it is possible the package may go back to the EUP for a second reading, in which case it is unlikely to be finalised till after the current French Presidency of the EU has rotated.

3. The EU Directives addressed by the Telecoms Package are:

    a. 2002/19/EC ('the Access Directive');
    b. 2002/20/EC ('the Authorisation Directive');
    c. 2002/21/EC ('the Framework Directive');
    d. 2002/22/EC ('the Universal Service Directive'); and
    e. 2002/58/EC ('the E-Privacy Directive').

4. The key documents referred to in this advice are as follows:

    a. Comm 2007/0247. This is the proposal for a Directive that would amend the Access, Authorisation and Framework Directives.
    b. Comm 2007/0248. This is the proposal for a Directive that would amend the Universal Service and E-Privacy Directives.
    c. TA (2008)0449. This is the consolidated list of amendments to Comm 2007/0247 adopted by the EUP on 24 September 2008.
    d. TA (2008)0452. This is the consolidated list of amendments to Comm 2007/0248 adopted by the EUP on 24 September 2008.
    e. CoM Auth 16 Oct 08. This is the proposal of the CoM regarding the text of the Authorisation Directive.
    f. CoM USD 10 Oct 08. This is the proposal of the CoM regarding the text of the Universal Service Directive.
    g. CoM FW 23 Oct 08. This is the proposal of the CoM regarding the text of the Framework Directive.
    h. Comm 247 6 Nov 08. This is the EU Commission's latest proposal regarding the text of the Directive to amend the Access, Authorisation and Framework Directives.

i. Comm 248 6 Nov 08. This is the EU Commission's latest proposal regarding the text of the Directive to amend the Universal Service and E-Privacy Directives.

5. It will be apparent from the above list that multiple versions of the texts in question are discussed in this analysis. In particular, there are three different amended versions of each of the additional Amending Directive: that agreed by the EU Parliament (the 'EUP Version'); that proposed by the Council of Ministers (the 'CoM Version') and the most recent response to these from the EU Commission (the 'Revised Commision Version'). Note also that the CoM addresses elements of the Directives in separate documents.

6. When reading these documents it is important therefore to be aware of the form in which they are presented. Documents (a) and (b) are draft Directives which consist of amendments to the existing Directives together with explanatory Recitals. Documents (c) and (d) are lists of amendments to (a) and (b), and thus are in large part 'amendments to amendments' so have to be read with care. Nonetheless, they are very comprehensive and clearly indicate where material has been added, amended or deleted. Documents (e), (f) and (g) however are in a rather different format, presenting the text of the Articles of the original Directives, as amended by the original amending Directive, the EUP changes to the amending Directive, and the CoM's own changes. Although textual formatting is used to indicate the source of such changes, it soon became clear that in many cases the CoM document does not indicate where changes made by the EUP have been discarded. In particular, large additions made by the EUP, such as the proposed Art.32a of the Universal Service Directive regarding protection against sanctions without due process of law, are absent from the CoM final text without any indication that any material has been deleted. I refer to this as 'implicit deletion' in my analysis. Finally, documents (h) and (i) comment in detail on the changes to the text of (a) and (b) as made by the EUP, with the Commission's responses and comments.

7. We have approached this analysis on the basis that there are two main areas in which the EUP and CoM have made amendments to the Telecoms Package that are crucial to the question of connection sanctions: **warnings and information given to users** of communications systems and **the actual measures taken against them**.

**WARNINGS RELATING TO USE OF NETWORKS**

8. The first substantial reference to warnings is contained in Art.20 of the Universal Service Directive, which governs the information that must be provided to users in their contracts for service with telecoms providers.

9. Art.20 originally provided that users should be informed, both when a contract was made and regularly thereafter, of any limitations placed on access to or distribution of lawful content, or use of lawful services and applications (original Art.20(5)) and of their obligations to respect copyright (original Art 20(6)). The EUP deleted both of these provisions via Amendments 70 and 71 of TA (2008)0452 but restated their content elsewhere. The provision regarding content was moved to an expanded Art.20(2)(b) whilst the provision regarding respect for copyright was subsumed into a new addendum to Art.20(2) which states:

*The contract shall also include any information which may be provided by the relevant public*

*authorities for this purpose on the use of electronic communications networks and services to engage in unlawful activities or to disseminate harmful content, and on the means of protection against risks to personal security, privacy and personal data, referred to in Article 21(4a) and relevant to the service provided.*

This is much broader than the original Art.20(6) and also refers to information provided by 'the relevant public authorities', which is a concept amplified at Art.21(4) as discussed below. However, its scope is slightly narrowed by the revised Commission version, which deletes 'any' from its first line.

10. Art.20(2)(h) as originally stated required that contract specify the action that a provider might take in reaction to security or integrity incidents or threats. The scope of this provision should be considered in light of the requirements inserted as Art.4(1b) of the E-Privacy Directive by the EUP which, as discussed below, potentially include peer-to-peer ('P2P') software as such a threat. The EUP amended this provision to rephrase it so as to refer to the *type of action* that might be taken – a rather less specific mandate – but added a requirement via Amendment 66 of TA (2008)0452 that providers specify the compensation arrangements applying in the event of security or integrity incidents. This latter requirement is implicitly deleted by the CoM text of 10 October, from which it is absent. The significance of this is that a requirement to notify compensation arrangements meant that providers would have to highlight whether or not they offered such compensation and the circumstances under which it would have been paid.

11. Wheras Art.20 covered information to be provided when a contract was made, Art.21 covers information provided at other times. The EUP amended (via Amendment 75) what was Art.21(4) in the original text so as to add a requirement to advise users of changes to their terms of service regarding restrictions on their ability to access, use or redistribute lawful content. This appears to replace the original requirement at Art 20.(5) to remind users of such constraints on use 'regularly' with one to advise them when such constraints change. The CoM did not change this amendment, but it made other amendments that renumbered this point to Art.21(3).

12. The EUP also added (via Amendment 76) a new Art.21(4a), later renumbered by the CoM changes to Art.21(4). This obliged providers to **distribute information provided by national authorities regarding warnings about the use of communications networks to engage in unlawful acts or distribution of harmful content, with specific reference to infringement of copyright**. The CoM did not alter this requirement, but it did implicitly delete a provision that required the cost of such distribution to be borne by national authorities rather than providers (or, in practice, customers.) This provision stands in the latest revised Commission version.

13. However, in the revised Commission version, the provision re cost refund seems to have been reinserted. Also, a reference to this being without prejudice to the e-Commerce directive. This would seem to imply that ISPs would not only be refunded for providing "3 strikes" type notifications, but would also be given the security of protection from possible liability in respect of such personalised warnings, should they prove, eg, to be libellous.

14. What does this provision mean? The argument is that although it is clear the article can be used to further the distribution of public benefit information, eg, advice on how to stop viruses, it also potentially provides a mandatory mechanism whereby ISPs and similar can be required to send

out repeated personalised warnings about alleged infringement –the “strikes” portion of Sarkozy’s “3 strikes” regime. The original Commission-proposed text included Recital 12, which simply stated that customers should be kept informed of the actions a provider may take in response to security or integrity incidents. The EUP added new Recitals 12b and 12c, considerably amplifying this statement. Recital 12b restated the need to inform users about response measures to security incidents. Recital 12c went into great detail on the need for public authorities to produce and disseminate what it describes as ‘public interest information’ on the risks and issues arising from use of communications networks, including warnings regarding copyright infringement and the dissemination of unlawful content. This Recital states the need for such information to be provided to users both when a contract is made and at other times. Distribution with a contract is covered by Art.20, whilst distribution at other times is covered by Art.21.

15. Further amplification of this guidance was provided by the EUP via Amendments 12, 194, 190 and 14 which respectively introduced Recitals 14a, 14b, 14c and 14d. Of these, Recital 14b defined ‘lawful’ and ‘harmful’ as follows:

> *In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the relevant authorities of the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful or not.*

It went on to advise that the Universal Service Directive did not affect the ‘mere conduit’ provision of Directive 2000/31/EC (‘the E-Commerce Directive’) and furthermore noted that:

> *Directive 2002/22/EC does not require providers to monitor information transmitted over their networks or to take punitive action or legal prosecution against their customers due to such information, nor does it make providers liable for the information. Responsibility for any such punitive action or legal prosecution remains with the relevant law enforcement authorities.*

16. The CoM version of the Universal Service Directive implicitly deleted all of Recitals 14a to 14d and replaces them with a single Recital 14a which preserved most, if not all, of the content of the EUP’s Recital 14b:

> *In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the relevant authorities of the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful or not. The Framework Directive and the Specific Directives are without prejudice to Directive 2000/31/EC (Directive on electronic commerce), which inter alia contains a "mere conduit” rule for intermediary service providers, as defined therein.*

The guidance that definitions of ‘lawful’ and ‘harmful’ be decided according to existing legal frameworks and the due process of law remain, as does the statement that the Telecoms Package does not change the well-established ‘mere conduit’ rule. However, the element that disclaimed the requirement for monitoring of content and which emphasised that sanctions were

to be imposed by national authorities has been removed by the CoM. This will be addressed further in the discussion on connection sanctions.

17. It seems that the revised Commission version leaves Recitals 14a to 14d intact. However, it does delete 'law enforcement' from the last line of Recital 14b – this is highly important since it may have the effect of widening the scope of punitive measures from bodies governed by due process to a wider range of agencies. It is also possible (see below) that it might mean personal or traffic data retained by ISPs to protect against security issues (eg zombie machines on the network) might also later be sought in civil proceedings by private actors such as copyright enforcement agencies. As discussed below, such data might be unavailable otherwise due to the safeguards of the data retention Directive and other DP legislation.

18. The issue of warnings was also addressed by the EUP through Amendment 101, which introduced Art.28(2a) as follows:

> *Member States shall ensure that national regulatory authorities are able to require undertakings providing public communications networks to provide information regarding the management of their networks in connection with any limitations or restrictions on end-user access to or use of services, content or applications. Member States shall ensure that national regulatory authorities have all the powers necessary to investigate cases in which undertakings have imposed limitations on end-user access to services, content or applications.*

This requirement provided that service providers should inform users where they impose restrictions on content or services and, more significantly, that government regulators should be empowered to investigate such restrictions. This particular provision touches on issues of both warnings and sanctions, in that it required providers to advise users of measures such as restrictions on the use of particular applications and encouraged the investigation of such restrictions. Whilst the requirement to advise users arguably merely repeats the provision of Art.20(2)(b) the power regarding investigation of limitations was new and would have provided a powerful tool for the regulation of constraints that providers imposed, be it on their own intitiative or at the behest of other parties. However, this point was implicitly deleted by the CoM, and para 4.3 of the revised Commission version confirms that Amendment 101 was not accepted by the Commission either.

19. A final reference to warnings is at Art.33(2a), as inserted by the EUP via Amendment 112:

> *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 as far as appropriate promote cooperation between undertakings providing electronic communications networks and/or services and the sectors interested in the promotion of lawful content in electronic communication networks and services. That co-operation may also include coordination of the public interest information to be made available under Article 21(4a) and Article 20(2).*

This provision requires regulatory authorities to **promote cooperation between providers and 'the sectors interested in the promotion of lawful content'**. Given the specific reference to

Art.21(4a) (now Art.21(4)), that is a clear reference to material infringing copyright and so the 'interested sectors' evidently include rights-holders and their organisations. Such cooperation is noted as including (but significantly, not being limited to) the coordination of the public interest information referred to at Art.21(4) and Recital 12c. In view of both the implication in Recital 12c and the clear statement in Art.21(4) that such information be produced by national authorities, it is interesting that Art.33(2a) refers to it being 'coordinated' with providers and 'interested sectors'. Furthermore, para 4.1 of the revised Commission version confirms that Amendment 112 was accepted by the Commission.

**MEASURES RELATING TO CONNECTION SANCTIONS**

20. The first significant mention of measures relating to connection sanctions is at Art.22(3). The original text of the amending Directive referred to the power of national regulators to set minimum standards for Quality of Service ('QoS'). QoS in network engineering terms generally means parameters such as connection speed, responsiveness and error rate and it is normal for network providers to take a range of measures to maintain the QoS of their networks. Such measures are potentially controversial as they may include either segregation of traffic according to tariff or user class (so-called 'net neutrality' issues) or the use of measures to identify and restrict certain sorts of traffic that causes particular QoS issues, such as P2P file-sharing (so-called 'throttling'). Such measures do not necessarily require detailed investigation of the content of traffic, a measure which would itself tend to introduce delay and so worsen QoS, but can rather be achieved by inspecting packet headers to determine the source, destination and type of service of the traffic in question.

21. The EUP amended Art.22(3) via Amendment 193 so as to emphasise that any such measures to preserve QoS should ensure that the ability of users to access or distribute content or to run applications or services should not be unreasonably restricted. This amendment imposed an implicit duty to apply QoS measures in an equitable manner, i.e. not by maintaining QoS for some users by unreasonably restricting the use of the network by others.

22. However, the CoM version of the text is very different; it explicitly amends the original text of the amending directive but in the process implicitly ignores Amendment 193. The resulting version of Art.22(3) simply requires that regulatory authorities be able to set minimum QoS requirements on to providers, with no caveats regarding the consequences for users in terms of ability to access content or services. The Commission takes a slightly different approach in its revised version: it accepts but then edits Amendment 193 so as to again remove all reference to the requirement to ensure that the ability of users to access or distribute content or to run applications or services of their choice is not unreasonable restricted. Nonetheless, both the CoM and revised Commission versions significantly water-down the safeguards inserted by the EUP at Amendment 193.

23. Further scope for measures affecting users is provided by Art.33(2a), as discussed at para above. By stating that co-operation between providers and 'interested sectors' may *include* co-ordination of warning information, it implies that such co-operation may well extend to other measures. The scope of such measures is addressed in the Authorisation Directive, to which the original Amending Directive added a new point 19 to the conditions at Part A of Annex I which may be attached to a general authorisation to provide communications services to include compliance with national measures implementing Directives 2001/29/EC and 2004/48/EC.

24. Directive 2001/29/EC is the Copyright Directive. As well as the general IP rights laid down in this Directive, this reference was presumably to Art.9 on enforcement. Art.9(1) provides that:

> *Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.*

whilst Art.9(2) states that:

> *Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).*

The clear implication is that enforcement measures shall be appropriate and proportionate, and that non-criminal sanctions shall be by the bringing of an action, i.e. due process of law in a civil court.

25. Directive 2004/48/EC is the IPR Enforcement Directive. Art.3 states that:

> *(1) Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.*
>
> *(2) Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.*

Throughout the remainder of the Directive there are repeated references to 'competent judicial authorities' and 'proceedings'. Although Art.16 provides that "Member States may apply other appropriate sanctions in cases where intellectual property rights have been infringed" it is clear from Recital 28 that this is a reference to criminal penalties.

26. In summary, the 'national measures' referred to in the original point 19 were all required by the relevant Directives to be proportionate, equitable and applied under due process of law.

27. The EUP, via Amendment 121, deleted the new point 19 and inserted a new point 19a:

> *Transparency obligations on public communications network providers to ensure end-to-end connectivity, including unrestricted access to content, services and applications, in conformity with the objectives and principles set out in Article 8 of Directive 2002/21/EC, disclosure regarding restrictions on access to services and applications and regarding traffic management policies and, where necessary and proportionate, access by national regulatory authorities to such information needed to verify the accuracy of such disclosure.*

The revised Commission version dilutes this somewhat, substituting 'foster' for 'ensure' and

deleting references to unrestricted access to content, services and applications and also the access requirement for regulatory authorities.

28. This change removed all reference to measures to enforce the Copyright and IPR Enforcement Directives and instead referred to Art.8 of the Framework Directive. The relevant elements would presumably be that of Art.8(4)(g) as amended by the EUP via Amendment 61 (change in bold):

*(g) applying the principle that end-users should be able to access and distribute any lawful content and use any lawful applications and/or services of their choice and for this purpose contributing to the promotion of lawful content in accordance with Article 33 of Directive 2002/22/EC (Universal Service Directive).*

and **Art.8(4)(ga) as added by the EUP via Amendment 138:**

***(ga) applying the principle that no restriction may be imposed on the fundamental rights and freedoms of end-users without a prior ruling of the judicial authorities, notably in accordance with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information,*** *save when public security is threatened, in which case the ruling may be subsequent.*

29. Art.8(4) was further amended by the CoM, which deleted Art.8(4)(ga) and split the amended Art.8(4)(g) into two separate points:

*(g) applying the principle that end users should be able to access and distribute any lawful content and use any lawful applications and/or services of their choice;*

*(h) contributing to the promotion of lawful content in accordance with Article 33 of Directive 2002/22/EC (Universal Service Directive).*

30. In both the EUP and CoM versions there is an implicit conflict between the wording of the revised point 19a regarding "unrestricted access to content, services and applications" and that of Article 8(4)(g) of the Framework Directive regarding the right to "access and distribute any lawful content and use any lawful applications." We have one Directive stating unrestricted access as a principle, and another restricting this principle to 'lawful' content and applications.

31. The EUP addressed this issue by, via Amendment 61, making reference back to Article 33 of the Universal Service Directive and to the principle stated at Art.33(2a) of co-operation between providers and 'interested sectors'. As such the principle under the original point 19 of the Authorization Directive of compliance with existing measures for copyright and IP enforcement is replaced with a principle of allowing access to lawful content (and thus implicitly excluding unlawful content such as infringing material) and of invoking the new provisions in the Act.33 for 'co-operation'.

32. However, the new Art 8 (4(ga) as inserted by the EUP under Amendment 138 then laid down a principle that any action restricting use of a network (such as filtering or disconnection, allowed under point 4(g) because it does not relate to 'lawful' traffic) **must be in accordance with requirements of due process and fundamental rights**, thus repeating and arguably

emphasizing and strengthening the requirements for such safeguards in the original point 19's reference to the Copyright and IPR Directives.

33. The CoM proposal however effectively removed this important safeguard. In the Universal Service Directive, Art.33(2a) was further amended, implicitly removing the reference to "unrestricted access to content, services and applications." Evidently the CoM has addressed the conflict between the two Directives as noted above by deleting the more permissive principle. Even more significantly, it **deleted the new Art.8(4)(ga) of the Framework Directive as inserted by the EUP's Amendment 138. With this safeguard provision removed, then not only is the connectivity principle under the Authorisation Directive limited to 'lawful' traffic but the obligation for 'lawful' to be determined by due process in a proportionate and equitable manner has been excised.**

34. **In the latest revised Commission version, however, Amendment 138 is, in a further twist, reinstated.** It is accepted 'in principle' and is noted as providing a "useful restatement of the need to ensure the balancing of fundamental rights". This is definitely good news for those concerned about connection sanctions as it is one of the two key 'safeguard provisions'. It is also a clear endorsement by the Commission of a key safeguard inserted by the EP and rejected by the CoM. If this amendment is retained in the final version, it would make it highly dubious if an arrangement such as that contemplated in the UK MoU, where ISPs and rightholders between them might order disconnection, would be sufficient "due process" and therefore legal. The proposed French law relating to connection sanctions however has disconnection mediated through a quasi-judicial body, and so might be regarded as having sufficient elements of "due process" to met Amendment 138's requirements. **It is clear the final acceptance or rejection of this Amendment is critical.**

35. Going back to the CoM document, it also implicitly deleted the *second* safeguard for due process and human rights in this domain, inserted by the EUP, the entirely new Art.32a of the Universal Service Directive which was inserted by the EUP **via Amendment 166:**

> *Member States shall ensure that any restrictions to users' rights to access content, services and applications, if they are necessary, shall be implemented by appropriate measures, in accordance with the principles of proportionality, effectiveness and dissuasiveness. These measures shall not have the effect of hindering the development of the information society, in compliance with Directive 2000/31/EC, and* **shall not conflict with citizens' fundamental rights, including the right to privacy and the right to due process**.

**Para 4.3 of the latest revised Commission version of the Directive amending the Universal Service Directive confirms that this (unlike Amendment 138) was not accepted and is deleted.**

36. This, like Art.8(4)(ga) of the Framework Directive, was a crucial 'safeguard' measure inserted by the EUP that would again have clearly restricted any connection sanctions to those that were proportionate and implemented under due process of law. As matters stood after the CoM stage, the CoM had deleted *both* of these safeguard measures, in both cases via 'implicit' deletion, i.e. the EUP-inserted provisions are simply absent from the CoM text rather having been marked as being amended or removed. **However as noted above para 34, the Commission's latest version has rescued one safeguard, in Amendment 138; it does**

**seem peculiar that the Commission has endorsed this, but not Amendment 166, since both have the same policy goal.**

Do the Telecoms proposals provide a potential legal basis for sanctions such as disconnection, and degradation of service or filtering?

37. If the Telecoms Package has potentially had removed from it at least one safeguard *against* summary connection sanctions, even in the latest Commission version, what scope does it provide *for* such sanctions to be imposed? And do the Telecoms proposals provide a potential legal basis for sanctions *other than* disconnection, such as traffic slowing or filtering (both mentioned as potential sanctions against alleged filesharers in the recent UK MoU)?

Providers were **obliged in the originally proposed version of Art.4 of the E-Privacy Directive**, as supported by Recital 20, **to take suitable measures to protect the "security" and integrity of their networks,** and to provide information to users about vulnerabilities and remedies. The EUP then amended Art.4 via Amendment 122 to add points 1a and 1b, with 1a amplifying the detail of security measures to be taken. These include:

– **appropriate technical and organisational measures to protect the network and services against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability***;*

– *a process for identifying and assessing reasonably foreseeable vulnerabilities in the systems maintained by the provider of electronic communications services, which shall include regular monitoring for security breaches; and*

– *a process for taking preventive, corrective and mitigating action against any vulnerabilities discovered in the process described under the fourth indent* [i.e. the sub-para above] *and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.*

"**Appropriate technical and organisational measures**" are not defined in the Telecoms Framework. They might conceivably cover activities against suspected file sharers, such as traffic slowing or even general measures such as filtering out of copyright works on the network where they are suspected to be infringing copies.

38. In the EUP version, which amended the original proposal, these new elements worryingly opened up scope for taking steps against consumers' usage of their ISP network. Notably, the wording in the first sub-para *requires* that these measures include protection against 'unlawful or unauthorised usage' irrespective of whether it affects the network. The crucial phrasing is the use twice of the word 'or' in the first sub-para, so creating three separate reasons by which providers might be required to implement protective measures:

a. accidental, unlawful or unauthorised usage of the network and services; or
b. interference with the network and services; or
c. hindering of the functioning or availability of the network and services.

39. But these actions are only allowed to pursue the goal of network "security". (see para 37.) How

is that defined? The provision refers to the existing definition in the Regulation which established the European Network and Information Security Agency (ENISA) ie EC Regulation 460/2004; Art.4(c) of the Regulation defines network and information security as follows:

*"network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or* ***unlawful*** *or malicious actions that compromise the availability,* ***authenticity****, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems;"*

It is difficult how this definition of "security", clearly devised to cover threats such as hacking and DDOS attacks, can be stretched to include unlawful filesharing activity. However it is conceivably possible if one looks at the words emboldened above ("unlawful" and "authenticity"). Any contract of service with a provider is likely to make copyright infringement or similar activity 'unlawful', and perhaps "unauthorised". **However it is the view of the authors that this provision does not and should not cover such filesharing activity.**

40. In a *very worst case interpretation* where filesharing activity *was* held to come under ENISA 4(c) Art.4 providers would have been required, (not just empowered) to take "technical measures" (etc) to protecting against filesharing activity, irrespective of whether it actually posing a genuine security threat to the network. The combined effect of Amendments 122 and 181 was therefore *potentially* to allow providers, potentially at the behest of rights-holders, to define use of P2P services as an act hindering the functionality of the network, which could then be investigated by traffic analysis and dealt with through connection sanctions.

41. **However in the CoM version, the new elements of Art.4 were deleted, thus removing this potentially wide and worrying interpretation**. **In the latest revised Commission version**, **the CoM rejection of the wide phrasing of the EUP proposal, remains undisturbed. In other words, as matters stand, Art 4 does not seem to provide authority for ISPs to be required to take sanctions against filesharers under the guise of "technical or organisational measures**" **to protect the "security" of their network.**

42. A final worry concerns **traffic data retention**. EUP Amendment 181 inserted a new Art.6(6a) into the proposed revision of the E-Privacy Directive as follows:

*Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive****, traffic data may be processed for the legitimate interest of the data controller for the purpose of implementing technical measures to ensure the network and information security, as defined by Article 4 (c) of Regulation (EC) 460/2004*** *of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency 1 , of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment,* ***except where such interests are overridden by the interests for the fundamental rights and freedoms of the data subject. Such processing must be restricted to that which is strictly necessary for the purposes of such security activity.***

The latest revised Commission proposal retains this proposal but deletes the first sentence up

to just before the word 'traffic'. It seems possible that this provision if passed would allow retention of traffic data for periods beyond those allowed as maxima by the Data Retention Directive (which specifies a maximum retention period of 24 months and which has been implemented as a shorter maximum period by some member states eg in UK, one year for Internet data).

42., Conceivably, if the above-noted ENISA definition of security is used, in the file-sharing context, Art.6(6a) might allow traffic data retention and subsequent analysis for the purposes of detecting unlawful copyright infringing content on networks. The key issue is that this might allow invasion of privacy beyond the proportionate limits debated at length in the Data Retention Directive debates. German scholars especially fear this might allow a "blank cheque" for retention of data for unlimited periods – which might then conceivably be available for data-mining by , eg, copyright enforcement bodies in civil discovery proceedings, when the retention of that data was only ever originally authorised for attention by law enforcement and security bodies.

43, The relevance of this provision to "3 strikes" is however, the authors assert, limited, since what the copyright enforcement authorities would surely prefer is access to such data without having to go through costly, public and time-wasting civil proceedings. Indeed in countries such as the UK, copyright enforcers can already gain access to such data via such devices as *Norwich Pharmacal* orders (and indeed, often do). The only gain in such countries is that the data may conceivably be available for longer periods than even the Data Retention Directive mandates.

**SUMMARY**

44. The central issue discussed here relates to the current state of the Telecoms Package and the extent to which it allows or does not allow (or requires, or does not require) the disconnection of alleged file-sharers from the Internet, without the involvement of courts to assess the evidence for the possibility of error, and to provide protection for due process and fundamental rights .It is indubitable that the Telecoms Package also provides many important consumer friendly guarantees, but these are not the topic of this brief. In particular, we wanted to find out if the Telecoms Package, at its latest stage, still provides a potential guarantee of legality for the "3 strikes and you're out" legislation currently being implemented in France and of interest in some other member states such as, notably, the UK. The key parts of the argument above have been emboldened.

45. On the basis of our analysis it is clear that the package does, or at least can, provide a mandatory basis for the "warnings" part of a French-style connection sanctions law (the "strikes") (see para 12 of brief), and also potentially provides a means by which public CSPs (ISPs and the like) can be compelled by the national regulator to work with ("promoting cooperation") rightsholders to implement a disconnection scheme (the "you're out" – see para 19 of brief). Wording in various places of the latest version seems to confirm that this "co-operation" is a more extensive obligation than simply providing copyright-related public interest information.

46. This is a crucial set of obligations, about to be imposed on all of Europe's ISPs and telcos, which should be debated in the open, not passed under cover of stealth in the context of a vast and incomprehensible package of telecoms regulation. It seems, on careful legal

examination by independent experts, more than possible that such a deliberate stealth exercise is indeed going on. When passed, these obligations will provide Europe-level authority for France's current "3 strikes" legislation, even though this has already been denounced as against fundamental rights by the European Parliament, when it was made *clear* to them what they were voting for or against.

47. Importantly, two amendments originally inserted by the EUP did provide protection against non-judicial imposition of disconnection and other sanctions against alleged file-sharers, in particular Art.32a of the Universal Service Directive (see para 35 of brief) and Art.8(4)(ga) of the Framework Directive (see para 28 ). However, both of these provisions were deleted by the CoM, and did not appear in the CoM's proposed final text.

48. Somewhat unexpectedly, however, one of these "safeguard" provisions, Art 8(4) (ga) ,was in fact reinstated by the Commission in the latest version. Why both Amendments 166 and 138 were not so reinstated is unknown, but may relate to "horse trading" between the Commission, the Council of Ministers and the European Parliament to get the package passed during the Sarkozy Presidency of the EU. Whether (ga) will survive to the final version of the Telecoms Package is anyone's guess, but it is clearly a key defence for civil liberties and against "3 strikes", as it explicitly protects both the right to due process and the right to private life. This brief commends its re-inclusion and suggests that Amendment 166 also be reinstated.

49. Turning to sanctions other than disconnection, the EUP made amendments to Art.6(6a) of the Framework Directive, which required the taking of "technical and organisational measures" by public CSPs to protect the security of their network. These measures were undefined and might perhaps include traffic slowing or "management" of an alleged file-sharer's account; and even filtering out of allegedly copyright-infringing files. These amendments were damagingly wide, because the definition of "security" borrowed from the ENISA Regulation seemed potentially capable of being stretched by those with an interest to do so to cover unlawful file-sharing within its ambit. What seemed therefore to be a provision requiring CSPs to act in the public good to protect networks from threats like viruses and hackers, could in actual fact potentially be interpreted in a way where it might also require CSPs to implement damaging technical sanctions against alleged (but not proven) filesharers.

50. In the event, subsequent amendments by the CoM, retained in the latest Commission revised version, appear to have removed this particular worry. This is to be applauded. However at this stage there is still time for anything to be added back to the raft of proposals, hence the discussion has been retained herein.

51. It has to be emphasised that such an interpretation would require extreme stretching of the words to enable particular interests; nonetheless, history provides many examples of legislation being used to ends outside its nominal purpose but within its literal meaning (most recently, for example, the use by the UK Government of anti-terrorist legislation to freeze assets of Icelandic banks). Although EU legislation is mean to be interpreted purposively, this is of particular concern to countries, such as the UK, that have a history of transposing and interpreting EU legislation in a more traditionally literal manner.

52. Finally we reiterate that this brief has been prepared to give a legal, rather than a lobbying, perspective upon the telecoms package. Good European law cannot be made when sectoral agendas are hidden within nested sets of amendments, obscure definitions by reference, and

overly wide and vague terminology. The purpose of this brief has been to open up these obfuscated agendas to the light of day. The brief is based on the Telecoms Package state of play as at 12 November 2008. It will be updated as developments occur.

Simon Bradshaw
Lilian Edwards

12 November 2008