EDPS response to the Commission's Consultation on its Report on the application of IPRED

1. Introduction

1. This document provides a response to the Commission's Consultation on its Report on the application of the enforcement of intellectual property rights Directive ("IPRED"[1]), published on 22 December 2010 (hereinafter 'the Commission's Report' or "the Report")[2]. A Staff Working Document[3] accompanies the Report.

2. The bulk of the Report is devoted to the perceived challenges that internet has brought to the enforcement of intellectual property rights and how to address them. Different tools or mechanisms are used to share content on the internet, potentially involving unlawful exchange of material subject to copyright. Examples of such tools or mechanisms include P2P file sharing. The Report states that gathering evidence of alleged copyright infringements committed using these tools or mechanisms is challenging. More particularly, the Report depicts data protection and privacy laws as possibly interfering with the application of Article 8 IPRED, which allows information to be obtained on the identity of the infringer[4].

3. The Report does not formulate any concrete proposal to address the perceived problem other than calling for further evaluation and, "*if necessary, means to remedy the situation*" regarding the relationship between the right of information (*ex* Art 8 IPRED) and protection of privacy and data protection, arguably hinting at a need to relax data/privacy protections.

4. Lacking concrete Commission proposals, the EDPS has decided to contribute to the Consultation exercise with some reflections on the current framework to enforce on-line intellectual property rights ("IP rights") and possible changes to it[5]. This is structured as follows.

5. Section 2 describes the typical actions (technicalities and facts) carried out to enforce copyright on P2P networks. The legal framework that applies to enforcement of IP rights using P2P platforms is explained in Section 3. Enforcement in P2P networks was selected as an example, not only because it is often referred to as the predominant platform for content covered by copyright, but particularly because it is a helpful example to illustrate how data protection/privacy requirements apply in the different steps carried out towards enforcing IP rights[6].

---

[1] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, L195, 2004-06-02, pp.16 – 25.

[2] Report on the enforcement of intellectual property rights (COM(2010) 779.

[3] Analysis of the application of Directive 2004/48/EC on the enforcement of intellectual property rights in the Member States (SEC(2010) 1589), hereinafter referred to as "Staff Working Document".

[4] Article 8 also allows information to be obtained on, for instance, someone providing services used in infringing activities on a commercial scale.

[5] Obviously these comments only focus on the aspects of the legal framework that have an impact on the data protection and privacy of individuals.

[6] There are other mechanisms that can be used to exchange information, including copyright-protected content, such as web download, streaming, etc. Furthermore, enforcement of IP rights on the internet is also affected by other platforms such as on-line trading marketplaces which can be used to trade

6. Section 4 comments on the Commission's Report and queries some of its explicit and implicit conclusions. In doing so, the EDPS puts forward proposals to clarify the legal framework and address the perceived problems.

2. P2P networks: facts and enforcement steps

7. P2P technology is a distributed computing software architecture that enables individual computers to connect to and communicate with other computers. Thus, the technology enables internet users to share information, including copyrighted material stored in their own computer, with other internet users[7].

8. The **first phase** of enforcement of IP rights in P2P networks consists of gathering evidence of alleged infringements. Right holders need to collect *prima facie* evidence of possible infringements. To that end, they may join P2P networks, monitor suspected usage and then make specific downloads of copyrighted material in order to obtain the following: (i) proof that copyright material is indeed being made available; (ii) IP addresses of the sources from where they downloaded the content; (iii) time/date of the alleged infringement and, (iv) a record of activity showing that someone (using a given IP address) is engaged in infringement[8].

9. **The second step** consists in effectively linking the evidence to an alleged infringer. The evidence of alleged internet infringements does not reveal directly the identity of an individual. Instead, it relates to an IP address that can be linked to an individual with the collaboration of the Internet Service Provider ("ISP").

10. To make the link between the IP address and the individual using it, the right holder may request a court to order the ISP to release the identity of the holder of the IP addresses from which the sharing of the copyrighted material was done.

11. Under IPRED, a court must balance several considerations, including the scale of the alleged infringement and the rights to data protection and privacy of the suspected infringer. Having done so, it may order the ISP to disclose information relating to the subscriber of the IP address.

12. The actions described above, which are instrumental in enabling copyright holders to enforce their rights on the internet, if done within certain parameters, are not incompatible with the existing data protection legal framework, as will be demonstrated below.

3. The Current Legal Framework

---

counterfeited goods. Some of the issues raised in P2P platforms may be present when using these other mechanisms but not necessarily all.

[7] Each computer constitutes a peer and is both supplier and consumer of information.

[8] This description summarizes the main steps taken by private specialised companies to track online alleged infringements on behalf of right holders. Along these main lines there are many variants. However, in all cases, the main pattern seems to be the blanket monitoring for some period of time of sites and servers supporting online content sharing followed by the analysis of such data.

3.1. Monitoring and recording of suspected IP addresses by right holders

13. As illustrated above, broadly speaking, the enforcement of IP rights on the internet may entail the monitoring of P2P usage involving the collection of suspected individual's IP addresses by holders of IP rights. This constitutes personal data as defined under Article 2 of the Data Protection Directive[9].

14. Pursuant to Article 8(5) of the Data Protection Directive[10], data related to offences, criminal convictions or security measures (usually referred to as "judicial data") can be processed only under strict conditions as implemented by Member States. IP addresses, collected as illustrated above, are deemed by the Article 29 Working Party as judicial data. While some variations may exist from one Member State to another, generally speaking, such data may only be processed to establish, enforce, or defend a legal claim.

15. However, Article 8 read together with Article 6(c) of the Data Protection Directive, requiring that processing be limited to what is "adequate, relevant and not excessive", put limits on the scope of the monitoring in terms of its scale and in terms of the amount of data collected and further processed. The Data Protection Directive must be interpreted in the light of Article 8(2) of the European Convention on Human Rights ("ECHR") and with Article 8 of the Charter of the Fundamental Rights of the Union. This also puts emphasis on the requirements for the processing to be necessary and to be in a reasonable proportion to the legitimate aim pursued. The above means that the processing must be carried out in the context of *specific*, current or forthcoming, judicial proceedings to establish, make or defend legal claims. Generalized monitoring followed by the storage on a general scale for the purpose of enforcing claims, such as the scanning of the internet as such or all the activity in P2P networks, would go beyond what is legitimate[11].

16. In addition, the Data Protection Directive provides additional conditions for legitimate data processing. These conditions are applicable to the processing of IP addresses described above. For example, those included in Article 6 of the Directive related to data quality *ex* Article 6(1)(d)[12], the conservation principle *ex* Article 6(1)(e)[13] and the purpose specification principle *ex* Article 6(1)(b)[14].

17. Moreover, some Member States have relied on Article 20 of the Directive[15] to require a prior check or authorization before the data collection can be carried out[16]. Given

---

[9] See also paragraph 27 of the EDPS Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA).

[10] 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 (hereinafter "Data Protection Directive"). L 281, 1995-11-23, pp.31 – 50.

[11] See footnote 9. Such a generalized monitoring by private entities has been declared unlawful by the Italian Data Protection Authority.

[12] It requires personal data to be accurate and kept up to date.

[13] It provides that data must be made anonymous or erased when it is not longer necessary for the purposes for which the data was collected.

[14] It requires personal data to be collected for specified, explicit and legitimate purposes.

[15] Article 20 enables Member States to determine data processing operations that are likely to present specific risks to the rights and freedoms of individuals and to require that these processing operations are subject to prior checking.

the sensitivity of the collection of such information, such an approach should be required.

18. Once having collected the IP addresses (and the information described under Section 2), right holders need to ascertain the identity of the holders of those IP addresses from ISPs pursuant to the conditions described below.

3.2. Storage and further processing of IP addresses by ISPs

19. The enforcement of IP rights requires the cooperation of ISPs, since they may have stored information on the individual using a given IP address identified by the right holder. Their cooperation is needed in order to identify the individual.

20. A relevant question is whether ISPs have a real need and the legal grounds to keep the records for the above mentioned purposes linking individuals to given IP addresses used for a certain communication. Pursuant to the ePrivacy Directive, ISPs may be allowed to store and further process IP addresses used by individuals after the communication has ended. However, the ePrivacy Directive sets limits to it, due to the sensitivity of information involved in communications activities. Concretely, ISPs may retain IP addresses data for billing purposes *ex* Article 6 of the ePrivacy Directive for such limited period of time during which the bill can be challenged, although in many cases this would not be necessary as the prevalence of flat rates[1] limits the cases where ISPs may legitimately store IP address usage for billing needs.

21. In addition, Member States, under the conditions set out in Article 15(1) of the ePrivacy Directive, can adopt legislative measures obliging providers to retain data. Such an obligation to retain data is contained in the Data Retention Directive[17] which requires ISPs to retain IP addresses for a limited period of time[18]. The disclosure of that information is however limited to competent national authorities for *the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law*[19]. Serious crime does not necessarily include copyright infringements[20].

22. It follows from the above that ISPs may at the time of receiving a request for the information either have the necessary data to link an individual subscriber to a particular IP address or not. However, the mere fact that ISPs have data available for a specific purpose (for billing purposes, or pursuant to an obligation of additional storage in the context of fighting serious crime) does not mean that these data can be

---

16 Such type of prior checking, followed by permits, is (or has been) required in countries such as France, Norway and Sweden. In the three countries, permits were requested (and granted or not) to engage in some data processing to counter illegal copying. In Sweden, the requirement for a permit was abolished through the transposition of IPRED.

17 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 networks, L105, 2006-04-13, pp. 54-63.

18 These comments do not address the question of whether the retention of traffic and location data of all persons in the EU is necessary and justified. The EDPS has dealt with these issues in other contexts. See for example, the EDPS Press release of 3 December 2010 entitled "The moment of truth" for the Data Retention Directive: EDPS demands clear evidence of necessity".

19 See Article 4 of the Data Retention Directive. This is without prejudice of Member States being able to derogate from the principle of confidentiality of communications for other purposes in application of Article 15(1).

20 Currently there is no harmonized EU definition of 'serious crime.'

transferred to copyright holders for another purpose. The next section analyses under what conditions the disclosure of data could be allowed.

3.3. Processing of requests and transferring personal information in the context of civil and criminal litigation

23. Pursuant to Article 15(1) of the ePrivacy Directive, Member States may adopt legislative measures obliging providers of electronic communications to cooperate with the authorities in the context of investigation, detection and prosecution of criminal offences. These measures must be in accordance with EU law. Pursuant to Article 8.2 ECHR, such measures should be necessary, appropriate and proportionate. In the case in hand, this means that ISPs may be ordered to disclose the identity of holders of IP addresses to judicial authorities in the context of criminal litigation, under the conditions foreseen by national legislation.

24. In addition to the above, in applying the Promusicae judgment of the ECJ[21], Member States may also lay down a legal obligation to disclose personal data in the context of civil litigation. This has to be read in conjunction with Article 8 IPRED, which obliges Member States to enable courts to order third parties, including ISPs, to provide information on alleged infringers when the alleged infringement has been conducted on a commercial scale[22].

25. Article 8 IPRED sets forth in itself some minimum requirements that limit the circumstances under which information must be disclosed. Namely, the requirement for a "commercial scale infringement", the requirement for the disclosure to be "in the context of proceedings" and the need for the request to be "justified and proportionate". It is then up to courts, on a case-by-case basis, to assess the facts, the gravity of the alleged wrongdoing, i.e. its scale and the privacy risks to individuals in order to make a decision as to whether to order or not the disclosure of information.

26. It follows from the above that the requirements for the initial monitoring of IP addresses to be necessary, proportional (ex Article 6.1(c) and Article 8 of the Data Protection Directive) are fully consistent with the proportionality, justification and commercial scale criteria that govern the disclosure of information under Article 8 IPRED.

4. Commission's Report in the Light of the Existing Legal Framework

4.1. A fair and reasonable legal framework to be maintained

27. All in all, the legal system described above, properly transposed, contains checks and balances intended to ensure that enforcement, civil and criminal, is possible without unduly jeopardizing individual privacy and data protection rights. It provides right

---

[21] *Promusicae v Telefonica* C-275/06; See par. 54 of the judgment.

[22] The "commercial scale" criterion is taken from Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), concluded on 15 April 1994 and signed by all the members of the World Trade Organization. It encompasses cases which cause significant harm to the right holder.

holders with means to establish infringements, criminal and also civil. Article 15 of the ePrivacy Directive – as explained by the ECJ in the Promusicae case - allows Member States to provide for a possibility to order ISPs to disclose the identity of holders of IP addresses also in the context of civil litigation. A correct transposition of Article 8 IPRED would require that Member States, in fact, allow for that possibility.

28. At the same time, the means available to copyright holders are not unlimited. Limitations are the logical result of the application of fundamental rights and the rule of law in democratic societies[23]. Accordingly, disclosure of individuals' identities will only take place when the alleged infringement reaches a commercial scale and the applicant has provided to courts sufficient evidence of the alleged infringement. The gravity of the wrongdoing and the considerable harm to the right holder favors, in such cases, giving weight to the provision of information on the identity of the infringer. The privacy and data protection rights should prevail when the conduct does not reach this threshold.

29. The EDPS considers that the system as a whole provides the appropriate checks and balances. More particularly the 'commercial scale' embodied in IPRED, pursuant to which the right to information in principle prevails, is welcomed. This, together with the need for the requests to be justified and proportionate and in the context of proceedings, are appropriate criteria to set the limits of when the right to ascertain the identity of individuals must prevail over the right to personal data.

30. The Commission's Report calls for special attention to the relationship between the right of information and the protection of privacy. It appears to suggest that changes to legislation on this aspect may be considered.

31. In principle, the EDPS does not favor changes to Article 8 IPRED for the reasons explained above and below. However, if changes were to be proposed, the EDPS would urge the Commission to avoid any distortion to the balance that exists in the current legal framework. More particularly, the EDPS calls upon the Commission to consider the following:

a) Ensuring due process and involvement of courts

32. The Report seems to indicate that ISPs should disclose personal data before judicial proceedings have started, and thus without a court order[24]. This would be contrary to Article 8 IPRED, which provides the exclusive mechanism for right holders to obtain information. Under Article 8 only "competent judicial authorities" may order the disclosure of the information, subject to a balancing test. The involvement of judicial authorities is an essential part of the current system and crucial to ensure that enforcement takes place in respect of due process and fundamental rights as well as of specific guarantees for the freedom and confidentiality of communications provided by constitutional charters in some Member States.

33. Furthermore, voluntary disclosure of personal information by ISPs without users' consent would also be in breach of the ePrivacy Directive.

---

[23] *Promusicae v Telefonica* C-275/06, See par. 68 and 69.

[24] See page 12 of the Staff Working Document.

b) Maintaining the right balance of interests

34. The Commission's Report avers that data protection and privacy challenge the application of the right of information under IPRED. This is despite the fact that, as the Report recognizes, experience in applying the Directive is limited and only few court cases have been reported. The Commission then appears to advocate for a different balance to be struck between the right to intellectual property and the rights to privacy and data protection.

35. However, the Report has no concrete suggestions on how to strike such a new balance. While not explicitly said, the Commission's solution in both the Report and the Staff Working Paper seems to appear as ambiguous and to point towards allowing or facilitating the unrestricted transfer of individuals' identities from ISPs to copyright holders[25].

36. As described above, Article 8 IPRED contains requirements enabling disclosure when the enforcement relates to an alleged wrongdoing on a commercial scale, disclosure is requested in the context of proceedings, and the information request is "justified and proportionate". However, arguably, the Commission seems to want to abandon some of these criteria. Instead it appears to favor the disclosure of personal information, i.e. the identities of individuals and/or IP addresses used by them, also in minor cases. This is contrary to the legislators' intention when the Directive was enacted, as interpreted by the Commission FAQ which said that the Directive "is not aimed at allowing the prosecution of large numbers of individuals using peer to peer networks for casual file swapping"[26]. It is also contrary to Recital 14 of IPRED which comments on the commercial scale criterion and more particularly says "this would normally exclude acts carried out by end consumers acting in good faith".

37. These criteria were adopted in 2004. The Report seems to imply that they may be outdated. It states in its conclusions that "it has become apparent that the Directive was not designed with the challenge posed by the Internet to the enforcement of intellectual property rights in mind". However, in 2004, the internet phenomenon was already in place with around 43% of the households connected to internet and around 15% of households with broadband[27]. The exchange of information, including alleged unlawful exchange of copyrighted content using P2P networks had existed already for some time, and was in fact a motivation behind IPRED as is

---

[25] In this sense, see various statements from the Staff Working Document which all seem to point in the direction of enabling systematic transfer of information on individuals to copyright holders. For example, "The possibility of intermediaries to share the data with the right holders would be an important element in this context". "The situation is more complicated if the request for information is made before the start of judicial proceedings", which clearly indicates a transfer without the involvement of courts. The following also suggest the need for transferring data before a court order (in order to facilitate showing evidence of the scale of the infraction: "At the same time, it appears that some right holders find it difficult to establish that the infringer has acted on a commercial scale without having obtained information from the Internet service provider, in particular on different IP addressees used by the same infringer". Also "In those Member States where privacy laws currently prevail over the right to (intellectual) property it can be difficult for the right holders to make effective use of their right of information". See also the Note on File Sharing from the European Parliament, Directorate-General for Internal Policies, Citizens' Rights and Constitutional Affairs, 2011, page 13 and 14, which shares the same perception.

[26] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/03/20&format=HTML&aged=&language=null&guiLanguage=en

[27] http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables

shown in the Commission's original proposal[28]. This confirms that the legislators took this into account and nevertheless set forth the current threshold. Recital 14 and Article 8 IPRED and the Commission FAQ confirm this view.

38. The criteria embodied in Article 8 IPRED are, to some extent, equivalent to the criteria that would otherwise apply under the ePrivacy and Data Protection Directives. Indeed, Article 8 IPRED encompasses the requirements of necessity and proportionality present both in the Directives and in the ECHR, which is an additional argument against changing it.

39. Furthermore, there is an enhanced danger that although, in the short term, new rules and criteria allowing unrestricted transfers of IP addresses to right holders may be considered as an effective enforcement tool, they are likely to become less helpful in the medium term. One should expect technical counter-measures to be developed to make the identification of IP addresses impossible or very difficult[29]. In practice, this would mean that a measure seriously invading the privacy of individuals would be adopted without any reassurance of a long term return.

40. In the EDPS view, a balanced approach should enable the co-existence of both rights (intellectual property and privacy). Furthermore, such an approach must respect the rule of law, due process and other fundamental rights. In the EDPS view, the current framework, properly implemented, delivers these guarantees and provides a proper balance. Thus, changes to it seem unnecessary.

41. However, the EDPS acknowledges that a balanced legal framework does not necessarily mean that the framework is clear. In this case, as the Commission's Report states, the framework is indeed ambiguous. As further described below, the interrelation between various Directives and the way in which the criteria should be applied in practice could be further clarified. This would be particularly helpful to courts and it would assist towards creating a harmonized EU approach.

4.2. Clarification of the existing legal framework

42. The Commission's Report has correctly identified the relationship between the right of information (Art 8 IPRED) and protection of privacy and personal data as an area that presents uncertainties and thus may require legal clarification.

---

[28] See COM proposal, http://www.europarl.europa.eu/oeil/file.jsp?id=230622. For example, page 3 refers to "Increasing use of the Internet enables pirated products to be distributed instantly around the globe". P 11: "In the multimedia products industry, counterfeiting and piracy via the Internet are steadily increasing and, despite the relatively recent development of the web, already represent considerable losses". Page 12 reads: "Counterfeiting and piracy, which were once craft activities, have become almost industrial-scale activities. They offer criminals the prospect of large economic profit without excessive risk. In the context of the Internet, the rapidity of illegal operations and the difficulty of tracking the operations further reduce the risks for the criminal. Counterfeiting and piracy carried out on a commercial scale are even said to have become more attractive nowadays than drug trafficking, since high potential profits can be obtained without the risk of major legal penalties".

[29] For example, the technology allows modifications of traditional P2P applications to enable anonymity. P2P applications can evolve to ensure that data is exchanged anonymously in a variety of ways such as not using application IDs or enabling double secured hops for every portion of bytes exchanged. It is also possible to use VPN (Virtual Private Network) hiding services so that ISPs could not link an IP address to a subscriber.

43. As shown above, the existing legal framework enables the establishment of infringements, criminal and also civil, without unduly jeopardizing individual privacy and data protection rights. However, the EDPS agrees with the Commission that the framework is not crystal clear. Several factors contribute to this. The framework is rather fragmented, because it is comprised of several Directives, which deal with different subjects, making the interaction between them not necessarily obvious. For example, the relation between Article 8 IPRED and the ePrivacy Directive is not apparent to everyone; the fact that Article 8 IPRED sets the conditions to provide individuals' data in response to court orders is not undisputed. The number of prejudicial questions to the ECJ that touches upon the applicable framework highlight that many questions remain open. Discrepancies in MS transposition may add to the confusion (see Section 4.3). This must be clarified. In addition to clarifying the interaction between the Article 8 IPRED and the ePrivacy Directive, clarification is necessary in the following two areas:

a) Setting clear limits to the allowed monitoring of internet users

44. As described above, enforcement of IP rights on the internet entails first the monitoring and collection of personal data, individual's IP addresses. Pursuant to Article 8 of the Data Protection Directive, such monitoring may be carried out in the context of specific, current or forthcoming, judicial proceedings. Blanket monitoring of individuals, in particular by private entities, would not meet the requirements of the law. In this regard, it would be useful to have clear guidance on the scope of the allowed monitoring.

45. Clarification on how to apply the framework and to make effective the balance of interests that it embodies would not only be useful but necessary. More concretely, it would be useful for copyright holders, but also for data protection authorities and courts to reach a common understanding on which type of monitoring would meet the criteria to be targeted and specific. Practical questions such as to what extent it is allowed to locate given trackers or links associated to copyright content and then monitoring the IP address sharing it should be discussed and clarified. Questions related to ascertaining repeat infringement are also relevant, for example, to provide evidence of commercial scale, as discussed below.

b) Ensuring a balanced approach to transferring subscriber details in the context of court proceedings

46. In addition to the above, practical, concrete, criteria may also be particularly helpful when national courts are confronted with requests for information. This would also contribute to a harmonized EU approach.

47. Discussion and guidance on the nature of the infringement and on the factors to establish the 'commercial scale' in P2P exchanges (and in other mechanisms) would be particularly useful in helping to weigh the interests of the parties. It may be relevant to give guidance on the conditions under which non-significant yet continuous infringements, over a period of time, for the purpose of commercial advantage or financial gain, would amount to 'commercial scale' and how to identify it. For example, P2P applications often have their own IDs, which may be helpful to

detect non-significant yet continuous infringements. They could potentially also be detected if IP addresses remain the same for a certain period (which is not unusual)[30].

48. Thus, the EDPS encourages the Commission to continue working on this area and would be pleased to contribute to this exercise.

4.3. Need to ensure an appropriate implementation of the applicable legal framework

49. The Commission's Report states that Member States' implementation of IPRED, but also of data protection and privacy legislation, may be preventing the effective exercise of the right to information (Article 8). The Staff Working Paper states that "*In some Member States .... it seems that the disclosure of the relevant information is practically impossible in both criminal and civil proceedings*". In this regard, in order to determine whether these practices infringe the *acquis communautaire*, the Report explicitly states that "*Further evaluations could be needed on the extent to which Member States' laws and the way they are applied are consistent with these requirements*". This seems to indicate that the Commission intends to analyze the compatibility of the existing Member State laws with the *acquis communautaire.*

50. The Commission has the duty to ensure that the Treaty and legal acts based on it, in this case, the relevant Directives, are upheld by the Member States. This can be done by launching infringement procedures under Article 263 TFEU. The EDPS fully agrees with the Commission's intention to bring Member States' transposition in alignment with the Directives and suggests that this should be a priority for the Commission.

51. The EDPS understands that in this case, the situation is quite complex. The Commission's evaluation of the implementation of the legal framework has to encompass not only IPRED but also the review of the other applicable Directives and ECJ decisions and the way in which they are *de facto* implemented. However, complexity should not be a deterrent for the Commission to act.

4.4. Need to explore alternative business models

52. The Report emphasizes that the internet and digital technologies present a challenge to the enforcement of IP rights. It also states that the widespread practice of file sharing of copyright protected content is due to the absence of a sufficient legal offer of digital content to keep up with demand. Such legal offers may in fact be largely absent in some Member States.

53. It follows from the above that the development of legal offers across the EU is likely to have a significant impact on the level of infringement and overall enforcement - monetisation - of IP rights. Despite this, neither the Report nor the Staff Working Document dedicates any comment on how to encourage the development of legal offers and how this would impact the perceived problems. Massive availability of bandwidth and ubiquitous connectivity should enable the development of e.g.

[30] More sophisticated methods exist:
http://hal.inria.fr/docs/00/47/03/24/PDF/bt_privacy_LEET10.pdf

streaming services both in the areas of music and films for very attractive fees. The rise of such new possibilities in the market could make less attractive the exchange of unlawful copyright material (in economic terms and also in terms of availability and quality).

54. The EDPS also regrets that no particular attention was paid in the Report to alternative economic business models, which may have much less privacy implications. For example, if copyright holders demonstrated their losses due to P2P usage, ISPs might provide differentiated internet access subscriptions, some with P2P access, others without. The part of the price for a subscription with unlimited access could be distributed to copyright holders.

55. These are areas that, in the EDPS view, would need further consideration and encouragement.

5. Conclusions and recommendations

56. In the EDPS view, the existing framework, correctly applied, provides an effective approach to enforcement while respecting the right to personal data and privacy. He is also of the view that the current Article 8 provides for an appropriate balance of rights and should not be modified. More particularly, he considers that:

- The commercial scale criterion should be maintained - while possibly clarified - as well as the requirement for the disclosure to be "in the context of proceedings" and the need for the information request to be "justified and proportionate".

- The need for court involvement in decisions about transferring personal data to copyright holders should be maintained. Upon the evaluation of the *prima facie* evidence provided by the right holders or law enforcement bodies, judicial bodies may order the transfer of personal data in the context of litigation in line with applicable law. Personal data should only be transferred in the context of civil litigation upon request or authorization of a judge who has evaluated the individual circumstances of the case. Other alternatives would unbalance the equilibrium between the two rights (intellectual property rights, data protection rights).

57. Despite the above, the EDPS agrees with the Commission that there is scope for improvement. In this regard, the EDPS welcomes that the Commission's Report brings forward possible suggestions for clarification. More particularly, he agrees that there is a need to clarify the relationship between the right of information (Art 8 IPRED) and the Directives related to the protection of privacy and data protection. The need for clarification also extends to other areas, outlined below.

- ***Issuing guidance on the limits to the allowed monitoring of internet usage***

58. Enforcement of IP rights on the internet entails first the monitoring and collection of personal data, individual's IP addresses. Pursuant to Article 8 of the Data Protection Directive, such monitoring may be carried out in the context of specific,

current or forthcoming, judicial proceedings. Blanket monitoring of individuals would not meet the requirements of the law.

59. In this regard, it would be useful to have clear guidance on the scope of the allowed monitoring. For example, copyright holders might engage in targeted monitoring of certain suspected IP addresses in order to prepare proceedings and verify the scale of the suspected violation. Today such monitoring seems to be a common practice, but it appears to be happening outside the legal data protection framework, including the proper supervision of data protection authorities.

60. This situation is clearly not satisfactory. The EDPS therefore proposes two set of actions: ***First,*** guidance setting forth allowed monitoring should be issued. Probably, the Commission, in consultation with the Article 29 Working Party would be well suited to carry out this task. Guidance would help to ensure the harmonized approach which is currently lacking. ***Second***, given the specific nature of this monitoring, it would be appropriate to subject this data processing to a prior check/supervision from data protection authorities. Authorities should analyze the methods and procedures and provide or deny authorization.

- ***Issuing guidance on how to ensure a balanced approach to transferring information (subscriber details) in the context of court proceedings***

61. Article 8 IPRED sets forth appropriate criteria under which courts may order the disclosure of the identity of alleged infringers in the context of civil and criminal litigation. As stated above, the EDPS considers that the current law provides for a careful, balanced approach which enables the enforcement of IP rights without impinging in a disproportionate manner upon individuals' rights to data protection and privacy.

62. However, the relation between Article 8 IPRED, the Data Protection Directive, the ePrivacy Directive and the Promusicae judgment should be clarified, for instance in an interpretative communication by the Commission. Such a communication could also serve as a basis for infringement proceedings against Member States which have not transposed EU law correctly. More particularly, practical guidance is needed in order to apply Article 8 IPRED in a way that balances the interest of the parties, ensuring that the criteria that it embodies and the balance of interests are well understood and applied.

- ***If changes were proposed, they must guarantee the protection of privacy and personal data***

63. If despite the above the Commission were to put forward proposals amending the current framework, it is essential to ensure that any changes to the existing law do not undermine an appropriate system of checks and balances, so that not only protection of the rights of copyright holders but also of privacy and data protection are guaranteed in the legal system.

Brussels, 8 April 2011