Are Internet protocol addresses personal data ?

Moiny, Jean-Philippe

Published in:
Computer Law and Security Review

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Are Internet protocol addresses personal data? The fight against online copyright infringement

Jean-Philippe Moiny

Research Centre in Information Technology and Law (CRID), FUNDP Namur, Belgium

Keywords:
Internet Protocol address
Data protection
Electronic communications
Online copyright infringement

ABSTRACT

Internet Protocol addresses [IP addresses] are central for Internet electronic communications. They individualize computers and their users to make the delivery of data packets possible. IP addresses are also often used to identify websurfers for litigation purposes. In particular, they constitute a key in the fight against online copyright infringement to identify infringers. However, it is a matter of dispute to know if IP addresses are personal data. In a review of relevant case law, the present paper seeks to identify when IP addresses are – or should be – considered as personal data. It suggests a contextual approach to the concept of personal data.

1. Introduction

A recent study has underlined that "in respect of the concept of "personal data" and "data subject", *important questions remain* about anonymisation and pseudonymisation, re-identifiability, *data on "things" that or linked to people (like IP addresses and traffic and location data)*, and "profiling". National laws and practices still give widely *differing answers* to these questions. […] [W]e fear that *these questions are still inadequately dealt with* at both EU-and national level"[1] (emphasis added by author).

The present paper seeks to clarify the status of Internet Protocol [IP] addresses[2] according to Directive 95/46/EC,[3] the general data protection Directive. The reasoning starts in Section 2 of the paper from the observations that IP addresses have to be identifiers of websurfers in the hands of Internet Access Providers. Section 3 considers how they are used to identify and sue websurfers. It then discusses in Section 4 different arguments against the status of IP addresses as personal data. In this respect, personal data is defined as " any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[4] In addition "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person".[5] Finally, in Section 5 of the paper consideration is given to the difficult issue as to when IP

[1] LRDP Kantor in association with Centre for Public Reform, Korff D, Brown I (core experts) et al. Comparative Study on Different Approaches to New Privacy Challenges, in particular in the light of Technological Developments. Final report delivered in the framework of contract JLS/2008/C4/011, European Commission, Directorate-General Justice, Freedom and Security, 20 January 2010, from http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, p. 28, [accessed 15.09.10]. The overall study is hereinafter referred to as "Comparative Study on Different Approaches to New Privacy Challenges".

[2] Save as otherwise stipulated, the paper refers to Internet Protocol version 4 [IPv4].

[3] 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, *O.J.* L 281, 23.11.1995, hereinafter referred to as "Directive 95/46/EC".

[4] Article 2, a) of Directive 95/46/EC.

[5] Recital 26 of Directive 95/46/EC.

0267-3649/$ – see front matter © 2011 Jean-Philippe Moiny. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2011.05.004

addresses have to – or should – be processed as personal data The ambit of the paper is not to be exhaustive, but it nonetheless refers to various case law from different – even non-EU – States.

2. IP addresses have to be identifiers

As traffic data, IP addresses fall under the confidentiality of electronic communication enshrined in Directive 2002/58/EC, the e-Privacy Directive.[6] This notably means that Internet Access Providers [IAPes] cannot reveal who are the parties to an electronic communication occurring through a public communication network.[7] However, Member States may adopt legislative measures to restrict the scope of this confidentiality of telecommunication data "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC.[8,9]" Especially, data retention duties exist at the European level (Section 2.1), and it can also be asked if such duties might be contractually provided (Section 2.2).

2.1. *Legal retention and access duties*

Firstly, European IAPes have data retention obligations according to Directive 2006/24/EC (Data Retention Directive)[10] and its national implementation. The Data Retention Directive provides derogation from the provisions of Directive 2002/58/EC dealing with confidentiality of electronic communications.[11] IAPes notably have to record the name and address of the subscriber or registered user and the allocated IP addresses.[12] This means that they make it possible to identify who made any electronic communication through their service. Of course, if IAPes have a data retention obligation,[13] they also have to give access to these data to the competent national authorities according to Member State's laws.[14] This processing of personal data[15] – *retention* and *communication* of data – are limited to a defined purpose: "the investigation, detection and prosecution of *serious crime* [grave *infractions*], as *defined* by each Member State in its national law".[16] The text of the Directive itself refers to *serious crime*, and some recitals illustrate it by quoting terrorism[17] and organized crime,[18] while recital 5 of Directive 2006/24/EC more generally refers to the investigation, detection and prosecution of *criminal offences*. Recital 9 is even broader referring to Article 8 ECHR and the purposes it provides as regards the possible limitations to the right to privacy. Data Retention requirements create an exception to the confidentiality of electronic communications and must be strictly construed. And a strict interpretation of the text of the Directive requires that the processing at stake have a purpose limited to the investigation, detection and prosecution of *serious crime* as defined by Member States. Moreover, rules establishing such processing have to "be accessible to the person concerned and foreseeable as to its effects".[19] Since criminal offences ("*infractions pénales*") cover numerous and varied behaviors (e.g.: defamation, assault, copyright

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *O.J.* L 201, 31.7.2002, hereinafter referred to as "Directive 2002/58".

[7] *See* Article 5.1 of Directive 2002/58/EC. As regards theses concepts, *see notably* Moiny J-P. Cloudy weather cloud based social networks sites: under whose control?. In: Dudley-Sponaugle A, Braman J, Vincenti G, editors. Investigating cyber law and cyber ethics: issues, impacts and practices. IGI Global, forthcoming 2011.

[8] "As regards the exception relating to unauthorized use of the electronic communications system, this appears to concern use which calls into question the actual integrity or security of the system", (ECJ, Judgment of the Court (Grand Chamber), January 29, 2008, *Promusicae v. Telefónica*, Case C-275/06, *European Court Reports* 2008, p. I-00271, no. 52).

[9] Article 15.1 of Directive 2002/58/EC.

[10] 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 and amending Directive 2002/58/EC, *OJ* L105, 13.4.2006, hereinafter referred to as "Directive 2006/24/EC". The Directive applies to "traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user" (Article 1.2 of Directive 2006/24/EC). Before the adoption of Directive 2006/24/EC, Member States laws generally already compelled IAPes to retention duties (now harmonized – to some extent – through the Directive).

[11] Article 3.1 of Directive 2006/24/EC.

[12] Article 5.1, (a), (2), (iii), and (c), (2), (i), of Directive 2006/24/EC.

[13] More precisely, data have to be retained to the extent they "are generated or processed by *providers of publicly available electronic communications services or of public communications network* within their jurisdiction in the process of supplying the communications services concerned", article 3.2 of Directive 2006/24 (emphasis added by author). As regards the services and networks at stake, see article 2.1 of Directive 2006/24 and article 2 (a), (c) and (d) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002, on a common regulatory framework for electronic communications networks and services (Framework Directive), *OJ* L 108, 24.4.2002, hereinafter referred to as "Directive 2002/21". *See also* Moiny J-P. Cloudy weather cloud based social networks sites: under whose control?. In: Dudley-Sponaugle A, Braman J, Vincenti G, editors. Investigating cyber law and cyber ethics: issues, impacts and practices. IGI Global, forthcoming 2011, footnote no. 179.

[14] Article 4 of Directive 2006/24/EC.

[15] The Directive applying to data related to legal entities, such data are not, *prima facie*, personal data according to Directive 95/46/EC since they do not relate to a living individual. *See infra* the developments related to Network Address Translation.

[16] Article 1.1 of Directive 2006/24/EC.

[17] Recitals 8, 9 and 10 of Directive 2006/24/EC.

[18] Recitals 7 and 9 of Directive 2006/24/EC.

[19] ECHR, Judgment (Grand Chamber), May 4, 2000, *Rotaru v. Romania*, Application no. 28341/95, no. 52. *See* nos. 55–56.

infringement, child pornography, unlawful parking, hacking, etc.), Member States have to define which of these behaviors are *serious* and therefore potentially mandate access to the retained telecommunications data by the competent authorities. As an example of an international definition of "serious crime", the United Nations Convention against transnational organized crime refers to a "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty".[20] Member States law must also define how long the above-mentioned data have to be retained by IAPes. This period has to last at least six months and up to two years at most, from the date of the communication.[21]

Secondly, since Article 15.1 of Directive 2002/58/EC refers to Article 13.1 of Directive 1995/46/EC, Member States can also derogate from the confidentiality of electronic communications for other purposes provided in this latter disposition.[22] For instance, one of these purposes is "the protection of the data subject or of the rights and freedoms of others".[23] In other words, derogations from Directive 2002/58/EC may also be adopted for *civil* and non-criminal purpose. In this respect, for instance, the confidentiality of telecommunications can be threatened for the purpose of fighting against copyright infringement. Member States are able – but not obliged[24] – to require a duty of disclosure of personal data in civil proceedings.[25] As regards the fight against online copyright infringement, Member States have to "reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other", to achieve a "fair balance" between these rights, and to respect the principle of proportionality.[26] It's always the same old song. As regards France for instance, the "HADOPI" statute[27] plans the processing of personal telecommunication data, a processing called "management system of measures for the protection of works on internet" ("*Système de gestion des mesures pour la protection des œuvres sur internet*"[28]). In this respect, IP addresses are precisely presented as the principal means to identify copyright infringers.[29]

Thirdly, as regards the data retention obligation, Article 15 of Directive 2000/31/EC (the E-Commerce Directive[30]) has to be pointed out. It specifies that: "Member States may establish obligations for *information society service providers* […] to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have *storage agreements*" (emphasis added by author). Referring to "information society services" involving "storage agreements", this obligation can therefore concern other providers than "electronic communications services" or "public communications network" providers.[31] Indeed, the definition of an "information society service"[32] (websites providers, web 2.0 platform providers, cloud computing service providers, etc.) is broader. For instance, while it can be considered that a social network site such as Facebook is not an electronic communications service according to Directive 2002/21/EC, it is clearly an information society service.[33] This retention obligation that Member States may impose on some information society service providers could be realized by requiring them to record the IP addresses used by their services' *users*. As mentioned above, since IAPes

[20] Article 2, b) of the United Nations Convention against Transnational Organized Crime adopted by General Assembly resolution 55/25 of 15 November 2000. In Belgium and France, for instance, copyright infringement is punishable – second offence and aggravating circumstances put aside – by a maximum deprivation of liberty of three years. Which do not meet the gravity of the cited definition of serious crime. *See* notably and respectively in Belgium and France, Articles 80 and 81 of the Loi relative au droit d'auteur et aux droits voisins du 30 juin 1994, M.B., 27 juillet 1994, and Articles L-335.2, L-335.3 and L-335.4 of the Code de la propriété intellectuelle.

[21] Article 6 of Directive 2006/24.

[22] *See Promusicae v. Telefónica,* ECJ 2008, no. 53.

[23] Article 13.1, (g) of Directive 1995/46/EC. *See also* Article 13.1 (d), (e) and (f) for other purposes than which that are specified in Article 15.1 of Directive 2002/58/EC.

[24] The Court ruled that article 8.1 of Directive 2004/48/EC (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, O.J. L 157, 30.4.2004), articles 15.2 and 18 of Directive 2000/31 (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), O.J. L 178, 17.7.2000, hereinafter referred to as "Directive 2000/31/EC") and articles 41, 42 and 47 of the TRIPS do not require Member States to lay down an obligation to communicate personal data in the context of civil proceedings, *see Promusicae v. Telefónica,* ECJ 2008, nos. 58–60.

[25] *Promusicae v. Telefónica,* ECJ 2008, no. 54.

[26] *Promusica v. Telefónica,* ECJ 2008, nos. 65–68. More recently, *see* ECJ, Order of the Court (Eight Chamber), February 19, 2009. *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH*, Case C-557/07, European Court reports 2009, p. I-01227.

[27] Loi no. 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, http://www.legifrance.gouv.fr/.

[28] *See* Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé "Système de gestion des mesures pour la protection des œuvres sur internet", available on http://www.legifrance.gouv.fr/.

[29] *See* Macrez F, Gossa J. "Surveillance et sécurisation: ce que l'Hadopi rate, A propos de la "petite loi" "Création et Internet". *Revue Lamy Droit de l'Immatériel,* no. 50, 2009, p. 85.

[30] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), O.J. L 178, 17.7.2000, hereinafter referred to as "Directive 2000/31/EC".

[31] *See supra* footnote no. 13.

[32] *See* Article 1, 2), a) Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, O.J. L 217, 5.8.1998.

[33] *See* Moiny J-P. Cloudy weather cloud based social networks sites: under whose control?. In: Dudley-Sponaugle A, Braman J, Vincenti G, editors. Investigating cyber law and cyber ethics: issues, impacts and practices. IGI Global, forthcoming 2011.

have to record which subscriber uses which IP address and when, during a period of at least six months, IP addresses can identify individuals. The recording of IP addresses could be deemed less intrusive than to require online identification through an electronic ID. It could also be considered more effective than to contractually require users to identify themselves by completing relevant fields on a webpage. For instance in France, Article 6.II of "LCEN" statute[34] compels providers of some online data storage services[35] to hold and keep data, ensuring the possibility of identifying anybody who contributed to the creation of content involved in these services. In this respect, waiting for a decree to specify the relevant data to retain, the *Tribunal de Grande Instance* of Paris has already deemed (in Magdane et al. v. YouTube (TGI Paris 2009)[36], Lafesse et al. v. Google et al. (TGI Paris 2009)[37] and J.F. v. SAS Networks (TGI Paris 2008)[38]) that the record of the users' IP addresses and their registration information (email addresses, names, etc., that can be fake, or temporary as regards the email) was sufficient to fulfill this obligation; IP addresses make it possible to identify the subscriber to the IA service.

2.2. *Contractual retention and access duties?*

In the end one wonders whether retention of electronic communications data could not be contractually provided. This could be useful to compensate for the lack of a Member State's national law in not explicitly allowing the processing of telecommunications data for the purpose of the fight against online copyright infringement. Indeed, with the unambiguous consent (defined by Directive 95/46/EC)[39] of all the *users*[40] – i.e. not necessarily the *subscribers* to the IA service at stake – involved in an electronic communication, then traffic data – and even content data – can be stored for a specific purpose and period of time.[41] In Ireland, as the case *EMI Records et al. v. Eircom* (IEHC 2010)[42] shows, Eircom tried to confine the online copyright infringement through a contractually based three steps procedure. This procedure can ultimately lead to the cut-off of recalcitrant users' Internet connection. Subscribers support the *effects* of the procedure by being identified via their IP addresses. Major companies (EMI Records, Sony, etc.) concluded an agreement with IAP Eircom setting the procedure. The measures taken against subscribers are legally based on the contract they concluded with the IAP.[43] The three steps procedure works as follows.[44] Production societies – or a hired computer agency such as DtecNet[45] – use software scanning the whole Internet (but focusing on Ireland) to identify IP addresses of websurfers illegally sharing copyrighted material over peer-to-peer networks.[46] Traffic and content relevant data (IP addresses, time, file shared, etc.) are then stored to be communicated to Eircom. On the first infringement, the subscriber identified through the IP address is told with his bill that a copyright infringement occurred as regards specific copyrighted material at a definite time. On a second infringement recorded and involving an IP address related to this same subscriber, a formal letter has then to be sent by Eircom. These two steps occur automatically. Finally on a third infringement notification, an Eircom employee is involved in the procedure (assessing the evidence at stake) and sends a termination notice. This latter informs the subscriber that his connection will be cut-off after 14 days. Of course, the cut-off knows some exceptions, and the subscriber is entitled to make representations to Eircom: representations that the IAP has to consider. In such a context, there is no doubt that that IAP Eircom (as regards rights owners or collecting societies, *see infra*) processes personal data.

As regards this particular kind of procedure, different remarks have to be made. Firstly, the data at stake relate to offences and as such have to be processed according to Article 8.5 of Directive 95/46.[47] This means that if they are not processed under the control of official authority – which is the case –, "suitable specific safeguards" have to be provided

[34] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (consolidée au 11 juillet 2010, retrieved on October 4, 2010, from http://www.legifrance.gouv.fr.

[35] For more precision as regards the definition of the targeted provider, *see* Article 6.I-2 of LCEN.

[36] Tribunal de Grande Instance de Paris, summary judgment (*ordonnance de référé*), March 5, 2009, *Magdane et al. v. YouTube,* retrieved on October 4, 2010, from http://www.legalis.net/. This question has not been contested on appeal, *see* Cour d'appel de Paris (Court of Appeal), 4th Chamber, Judgment, March 26, 2010, *YouTube v. Magdanes et al.*, retrieved on October 4, 2010, from http://www.legalis.net/.

[37] Tribunal de Grande Instance de Paris, 3d Chamber, Judgment, June 24, 2009, *Lafesse et al. v. Google et al.*, retrieved on October 4, 2010, from http://www.legalis.net/. *See* Trézéguet M. "Prestataires du web 2.0: l'adresse IP est une donnée personnelle". *Revue Lamy du Droit de l'Immatériel,* no. 51, 2009, pp. 47–48.

[38] Tribunal de Grande Instance de Paris, summary judgment (*ordonnance de référé*), June 23, 2008, J.F. v. SAS Networks, p. 4, retrieved on October 4, 2010, from http://www.juriscom.net/jpt/visu.php?ID=1089.

[39] "Save as otherwise provided, the definitions in Directive 95/46/EC […] shall apply" (Article 2, al. 1 of Directive 2002/58/EC). *See* Article 2, h) of Directive 95/46/EC.

[40] That is to say: "any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service" (Article 2, al. 2, a) of Directive 2002/58/EC).

[41] Article 5.1 of Directive 2002/58/EC.

[42] High Court (Ireland), Judgment, April 16, 2010, *EMI Records, Sony BMG Music; Universal Music and Warner Music. v. Eircom*, [2010] IEHC 108.

[43] There is of course a contract between any subscriber an Eircom, and this agreement provides that it may be suspended or terminated for breach of its terms, terms that forbid to create, host or transmit copyright infringing materials (*EMI Records et al. v. Eircom* (IEHC 2010), no. 14).

[44] *EMI Records et al. v. Eircom* (IEHC 2010), nos. 9–13.

[45] *See* http://dtecnet.com/.

[46] *See EMI Records et al. v. Eircom* (IEHC 2010), no. 20.

[47] See notably in the same sense, the position of the Belgian Privacy Commission, Avis d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les communications, n°44/2001, November 12, 2001; European Data Protection Supervisor, Opinion on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), O.J. C 147, 5.6.2010, nos. 51–52.

under national law. Secondly, traffic data are processed by production societies and the IAP while the consent of the *users* concerned by the electronic communications at stake is not asked. And yet, these consents are required according to Article 5.1 of Directive 2002/58 that limits the possibilities of using electronic communications and traffic data but of course, save as otherwise provided by national law legally derogating from the Directive. Thirdly, it could be imagined that the contract between the subscriber and the IAP contains the former's consent to the processing of the above-mentioned. For instance, the contract[48] could provide the following statement: "by subscribing to our services, you agree that traffic data will be stored and monitored for copyright infringement purposes as detailed *infra*, etc.". This contract could then further compel a subscriber to make any individual using his Internet access service to agree to such a monitoring of *his own use* – as a *user* – of the *subscriber*'s Internet access service (e.g. via a third-party beneficiary clause).[49,50] In these cases, our view is that the subscribers/users' consent would not be freely given because all IAPes of the relevant market would propose such agreements.[51] Subscribers/users would have no other choice than abiding to the processing. In other words, the processing at stake is not based on the subscriber/users' consents.

This finally leads to the following further consideration: if IAPes require their subscribers to agree that such IAPes can identify them vis-à-vis collecting societies (or right holders) when copyright infringements are alleged – which diverges from the Irish case above –, two difficulties arise. On the one hand, IAPes would still have to obtain the consent of users (when a user is not the subscriber), save as otherwise provided by national law (according to Article 15.1 of Directive 2002/58/EC). On the other hand, the consent of the subscriber would still not be freely given, whereas it should be.[52] To sum up, in our view, IAPes should not legally be able, contractually and generally, to identify their subscribers to the music industry, collecting societies, right holders or more generally legal claimants without a "legislative measure" of national law – clear, accurate, therefore predictable, and proportinate[53] – adopted according to Article 15.1 of Directive 2002/58/EC.

In conclusion, IP addresses allocated by "European"[54] IAPes *have, at least, legally to relate to* the subscribers of the IA services for a period of time that Member States have set (between six months and two years), for specific purposes that Member States have to define according to Directive 2006/24/EC and Articles 15.1 of Directive 2002/58/EC as well as Article 13.1 of Directive 95/46/EC.

3. Use of IP addresses to identify and sue websurfers

Because they constitute an identifier, IP addresses are processed to identify and to sue websurfers. IP addresses are keys to the identification of online copyright infringement. The fight against this kind of infringement has internationally existed for some time now depending on the country at stake. Clearly in this fight: "with the assistance of the ISPs, the cloak of anonymity can be pierced and the true identity of the infringers may be revealed".[55]

In *France*, the processing of IP addresses has already been used particularly *to sue* copyright infringement by individual up/downloaders and therefore *to identify* them. This occurred before the enactment of the HADOPI statute previously evoked. Agents of collecting societies (SACEM and SDRM) used software enabling file sharing over peer-to-peer networks to identify users sharing copyrighted works. They complained to

[48] It should also be underlined that if the collection of users' IP addresses and of the relevant linked pieces of information by collecting societies are to be considered a processing of personal data – which should be the case –, these societies should also be a party to the contract concluded between the IAP and its users. Otherwise, they would have to find another mean to get users/subscribers' consents.

[49] It has to be noted that consents of all users/subscribers concerned being required, an IAP could then only process data related to its own users/subscribers. In other words, both parties to the communication would have to be one of its subscribers. To allow the IAP to process traffic data when a user concerned by the electronic communication is a subscriber of another IAP, a third-beneficiary clause would be needed. Such a clause, for instance, would be stipulated in the contract between this other IAP and his users.

[50] The consent of *users* could also be more efficiently required, for instance, by the providers of software making it possible to share data through peer-to-peer network. However, when the user is not the subscriber to the IA service, IAP will not be able to process personal registration data because they will lack the consent of their subscriber to the processing at stake.

[51] "Since it was likely to be deeply unfair that only Eircom with about 40% of the market share, as the defendant in these proceedings, should bear the burden of this settlement, thus activating the winds of market forces to drive customers towards Eircom's competitors, the plaintiffs agreed to initiate similar proceedings against other internet service providers in the State" (*EMI Records et al. v. Eircom* (IEHC 2010), no. 10).

[52] And the processing of subscriber's personal data (here the application of Directive 95/46/EC is not questionable since the IAP knows the identity of his subscriber, *see infra* as regards other collectors of IP addresses) could not only be done in virtue of Article 7, f) of Directive 95/46/EC. Indeed, according to Article 5.1 of Directive 2002/58/EC, the consent of the concerned users is required for (notably) the storage of traffic data, save as exemption to this Article provided by national law according to Article 15.1 of Directive 2002/58/EC. For instance, since Member States can refer to the purposes set in Article 13 of Directive 95/46/EC (*see* footnote no. 22), they could specify that *a user* addressee of the electronic communication at stake (a website provider receiving a request to consult a webpage, an individual receiving an email, etc.) may store the content and traffic data of this communication without the consent of the other users concerned. Web 2.0 platform such as social network sites (Facebook, YouTube, etc.), webmail providers, etc., could also require the contractual consent of their users to store their IP addresses (taking the risk that it is not freely given), etc. If the IP address is considered to be personal data *per se*, then they will also have to obtain the consent of the subscriber to the IA service if they cannot rely on another ground according to Article 7 of the Directive 95/46/EC.

[53] See the criticism of the European Data Protection Supervisor as regards the proportionality of the three steps procedure, *op. cit.*, nos. 32–49.

[54] *See* Articles 1.1 and 3.1 of Directive 2006/24/EC.

[55] Court of First Instance (Hong Kong), January 26, 2006, *Cinepoly Records Co Ltd et al. v. Hong Kong* Broadband Network Ltd *et al.*, [2006] HKLRD 255, n°14.

the police that required IAPes to identify the subscribers behind IP addresses. Logging with the relevant software, the sworn agents noticed peers sharing protected works in their shared folders. Then they tested whether the shared files were downloadable and whether they were what their names specified them to be. To identify the IP addresses of these users and their IAPes, the agents relied on the software "VisualRoute", consulted the "WHOIS" databases and used the firewall "Kerio Personal Firewall". Finally, they burned these data and the relevant screen captures on a CD they sent to the police. The question arose before the French court to know whether this whole procedure amounted to the processing of personal data since such a processing should have been submitted to an authorization from the Commission Nationale de l'Information et des Libertés [CNIL] (the French privacy commission). In the cases submitted to courts, the sworn agents acted without CNIL authorization and therefore, the proof submitted should be deemed inadmissible in the initiated copyright litigations.

Numerous examples exist in the French case law where IP addresses are sometimes considered to be personal data or they are not. In two cases discussed later in this paper, *Anthony G. v. SCPP* (CA de Paris 2007)[56] and *Henri S. v. SCPP* (CA Paris 2007),[57] relating to "KaZaA", the Paris Court of appeals decided that IP addresses *were not* personal data. Therefore, the sworn agents did not need CNIL authorization. However, first instance courts had already concluded to the contrary. For instance, in *Laurent F. v. SACEM et al.* (TGI Bobigny 2006), the court previously considered in the same kind of litigation, related to "Shareaza", that IP addresses were personal data. It considered that such numbers establish the correspondence between the identifier allocated to the websurfer during the connection, and the identity of the subscriber.[58] In *SCPP and SACEM v. J.P.* (TGI Saint-Brieuc 2007), related to "Soulseek", IP addresses were personal data processed by the sworn agents. The court made an analogy with a phone number explaining that it is linked to a subscriber via the IAP.[59] The judgment had even been confirmed on appeal by the Rennes Court of appeals. But the decision was finally revoked by the Cour de cassation in *SCPP et al. v. J.P.* (Cass. Fr. 2009).[60] The Rennes Court of appeals, in *Cyrille S. v. SACEM and SDRM* (CA Rennes 2008),[61] also explicitly ruled that an IP address is an indirectly nominative personal data acquiring a nominative character through the mere connection with the database owned by the IAP. But this ruling has also been revoked by the Cour de cassation in *SACEM et al. v. Cyrille S.* (Cass. Fr. 2009).[62] In its two arrests, it is crucial to underline that the Cour de cassation did not ruled that IP addresses were not personal data. It avoided the question.[63] It rather decided that the sworn agents' behavior did not amount to a processing realized through *automated means*.[64] The Court specified that the agent at stake made "visual findings" ("*constatations visuelles*"), "manually" accessed the list of shared files and had not recourse to a "prior automated surveillance processing" ("*traitement préalable de surveillance automatisé*"). This has been recalled by the Paris Court of appeals, to which one of the cases had been remanded, in *Cyrille S. v. SACEM and SDRM* (CA Paris 2010).[65] Therefore, case law considering that IP addresses are personal data and offer the possibility to identify individuals is still valid.[66]

In a context similar to what happened in these French cases, *in Switzerland*, the Federal Supreme Court decided on 8 September 2010, that "IP addresses are clearly personal data and are thus subject to the Data Protection Act".[67]

In *Belgium*, in 2001, the Belgian Privacy Commission similarly pronounced itself. As regards the fight against copyright

[56] Cour d'appel de Paris, 13th Chamber, April 27, 2007, Anthony G. v. Société Civile des Producteurs Phonographiques (SCPP), retrieved on October 4, 2010, from http://www.legalis.net/.

[57] Cour d'appel de Paris, 13th Chamber, May 15, 2007, *Henri S. v. Société Civile des Producteurs Phonographiques* (SCPP), retrieved on October 4, 2010, from http://www.legalis.net/.

[58] Tribunal de Grande Instance de Bobigny, December 14, 2006, *Laurent f. v. SACEM et al.*, retrieved on October 4, 2010, from http://www.legalis.net/.

[59] Tribunal de Grande Instance de Saint-Brieuc, September 6, 2007, *Société Civile des Producteurs Phonographiques (SCPP) et Société des Auteurs, Composieteurs et Editeurs de Musique (SACEM) v. J.P.*, retrieved on October 4, 2010, from http://www.legalis.net/.

[60] Cour de Cassation, Criminal Chamber, June 16, 2009, *Société Civile des Producteurs Phonographiques (SCPP) et al. v. J.P.*, *see* L. Costes, "Téléchargement illegal d'oeuvres musicales et process-verbal de l'agent verbalisateur", *Revue Lamy Droit de l'Immatériel*, no. 52, 2009, pp. 16–18.

[61] Cour d'appel de Rennes, 3d Chamber, May 22, 2008, *Cyrille S. v. Société des Auteurs, Compositeurs et Editeurs de Musique (SACEM) and Société pour l'Administration du Droit de Reproduction Mécanique des Auteurs et Compositeurs de Musique* (SDRM), retrieved on October 4, 2010, from http://www.legalis.net/.

[62] Cour de Cassation, Criminal Chamber, January 13, 2009, *Société des Auteurs, Compositeurs et Editeurs de Musique (SACEM) and Société pour l'Administration du Droit de Reproduction Mécanique des Auteurs et Compositeurs de Musique (SDRM) v. Cyrille S.*, *8 Recueil Dalloz*, 2009, p. 497.

[63] In the same sense *see* Costes L. "Téléchargement illicite d'oeuvres : constatation de l'infraction et données personnelles". *Revue Lamy Droit de l'Immatériel*, no. 46, 2009, p. 22; Chafiol-Chaumont F, Bonnier A. "L'identification des "pirates du Web" à partir de leurs adresses IP, De la qualification du constat probatoire de l'agent assermenté mandaté par la SACEM au projet de loi "HADOPI". *Revue Lamy Droit de l'Immatériel*, no. 49, 2009, p. 86; Pignatari O. "Téléchargement illicite d'oeuvres musicales: l'articulation – toujours – delicate avec les données personnelles et le rejet persistant de la copie privée". *Revue Lamy Droit de l'Immatériel*, no. 60, 2010, p. 15 and the references quoted by the author in footnote no. 16.

[64] In the same sense, *see* notably Daleau J. note under Cour de cassation, crim., 13 janvier 2009, *8 Recueil Dalloz*, 2009, p. 497; Teller M. "Les difficultés de l'identité numérique: quelle qualification juridique pour l'adresse IP?". *Recueil Dalloz*, no. 29, 2009, p. 1990.

[65] Cour d'appel de Paris, 12th Chamber, February 1st, 2010, *Cyrille S. v. SACEM and SDRM*, retrieved on October 4, 2010, from http://www.legalis.net/).

[66] *See* also *supra* the case law of the Tribunal de grande instance de Paris as regards data retention obligations.

[67] Federal Data Protection and Information Commissioner (Switzerland), http://www.edoeb.admin.ch/aktuell/01688/index.html?lang=en, last visited on October 7, 2010. *See also* the press release of the Federal Court (September 8, 2010), http://www.bger.ch/fr/mm_1c_285_2009_d.pdf, [accessed 14.12.10]. The decision (cases nos. 1C_285/2009 and 1C_295/2009) is published in German language on http://www.bger.ch.

breaches, it specifies that the processing of – static or even dynamic – IP addresses must submit to data protection law in so far as it is possible – "and easy" – to find the identity of the individual concerned through the intermediary of the IAP.[68] And in this respect, it does not matter that the right holder has knowledge of the data, and that he is not authorized to know these data. The advice of the Commission targeted what the International Federation of the Phonographic Industry [IFPI] did, that is: noticing the IP addresses of users using Napster and related networks. More recently, in 2008, the IFPI registered in Belgium its processing of websurfers IP addresses for litigation purposes.[69] In any case, the identification of websurfers is necessary to the fulfillment of the purpose pursued by IFPI and, more generally, collecting societies, etc.

In the *United States of America*, on the one hand, the Recording Industry Association of America [RIAA] began to fight against individual infringer seven years ago.[70] To identify infringers, the RIAA followed the same kind of practical steps as French collecting societies. It was for instance the case in *RIAA v. Charter Communications* (8thCir. 2005),[71] where the "KaZaA" and "iMesh" shared peer-to-peer network was at stake. *Maverick Recording et al. v. Whitney Harper* (5thCir. 2010)[72] illustrates the role of the MediaSentry company in the tracking of websurfers for the RIAA. On the other hand however, online copyright litigation infringement has not always been directed against websurfers. It is notably referred to the well-known "Napster", "Grokster" and "StreamCast", and "Aimster" cases. More recently, in *Columbia Pictures et al. v. Justin Bunnell et al.* (C.D. Cal. 2007),[73] the "Torrentspy" website was at stake. This is "a website that serves as a search engine that enables users to locate and download dot-torrent files".[74] The website administrators' responsibility was discussed. What was interesting for the present purpose is that the district Court ruled that "[e]ven if the users are engaged in *legal* file sharing, they have little to no expectation of privacy because they are broadcasting their identifying information to everyone in the BitTorrent "swarm" as they download the file".[75] *A fortiori*, they neither have reasonable expectation of privacy while infringing the copyright of others. In this case, in a previous order, Justice Chooljian requires the website administrators to record "server logs". These included the IP addresses of the website users who requested dot-torrent files. The aim of this order was to make it possible to assess the potential website administrators' responsibility as regards copyright infringement made by the users. If users have no expectation of privacy as regards what they broadcast, it is nonetheless enlightening to note that the judge required that IP addresses, in a nutshell, be "encoded".[76] In doing so, Justice Chooljian therefore clearly took into account the potential later litigation that could be directed against these users with the help of their IP addresses.

Coming back to Europe, as the *Working Party 29* wrote: "to argue that individuals are not identifiable, where the *purpose* of the processing is precisely to identify them would be a sheer contradiction in terms"[77] (emphasis added by author). In the "French-like" instances, the Working Party 29 explicitly considers that a processing of personal data is at stake. He wrote: "in those cases where the processing of IP addresses is carried out with the purpose of identifying the users of the computer (for instance, by copyright holders in order to prosecute computer users for violation of intellectual property rights), the controller anticipates that the "means likely reasonably to be used" to identify the persons will be available e.g. through courts appealed to (otherwise the collection of the information makes no sense), and therefore the information should be considered as personal data".[78] In a same sense, as P.J. Hustinx (European Data Protection Supervisor) also wrote, the above-mentioned rulings of the Paris Court of Appeal relating to the status of personal data

[68] The Commission underlined that this identification of individuals is *necessary* to the fulfillment of the objective pursued – in the case – by the IFPI, that is to say to take proceedings against the individual who have the IP addresses at stake. Commission for the protection of privacy (Belgium). Avis d'initiative concernant la compatibilité de la recherché d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, n°44/2001, November 12, 2001, p. 3. The advices of the Belgian privacy commission (CPVP) are available on http://www.privacycommission.be.

[69] See the Belgian public register of processings, https://www.privacycommission.be/elg/publicRegister.htm?decArchiveId=32072, declaration made by IFPI Belgium, and published form the 22 January 2008.

[70] *See* Electronic Frontier Foundation, "RIAA v. The People: Five Years Later", September 2008, retrieved on October 5, 2010, from http://www.eff.org/riaa-v-people. For a thorough study in the United States as regards IP addresses, *see* J.J. McIntyre, "The number is me: why internet protocol (IP) addresses should be protected as personally identifiable information", *DePaul Law Review*, no. 60, 2011, forthcoming, retrieved on http://www.ssrn.com.

[71] U.S. Court of Appeals for the Eight Circuit, April 1st, 2005, *The Recording Industry Association of America v. Charter Communications*, p. 5, from http://www.ca8.uscourts.gov [accessed 04.10.10].

[72] U.S. Court of Appeals for the Fifth Circuit, February 25, 2010, *Maverick Recording Company et al. v. Whitney Harper*, no. 08-51194, pp. 2–3, from http://www.ca5.uscourts.gov/ [accessed 04.10.10].

[73] US District Court for the Central District of California, June 19, 2007, *Columbia Pictures et al. v. Justin Bunnell et al.*, U.S. Dist. LEXIS 46364, from http://www.eff.org/files/filenode/torrentspy/20080814%20judgment.pdf [accessed 07.10.10].

[74] *Columbia Pictures et al. v. Justin Bunnell et al.* (C.D. Cal. 2007), p. 2, lines 4–5.

[75] *Columbia Pictures et al. v. Justin Bunnell et al.* (C.D. Cal. 2007), p. 15, line 10.

[76] Justice Chooljian ordered that "defendants shall mask, encrypt, or redact IP addresses through a hashing program or other means, provided, however, that if a given IP address appears more than once, such IP address is concealed in a manner which permits one to discern that the same IP address appears on multiple occasions"; and she specified that "Plaintiffs are prohibited from using "brute force" or any other means to pierce or reverse any such mask/encryption/redaction" (U.S. District Court for the Central District of California, Magistrate Order, May 29, 2007, *Columbia Pictures et al. v. Justin Bunnel et al.*, no. CV 06-1093 FMC(JCx), p. 34, lines 3–12, from http://www.eff.org/files/filenode/torrentspy/columbia_v_bunnell_magistrate_order.pdf [accessed 04.10.10].).

[77] WP136, p. 16.

[78] WP136, p. 17.

"do not seem to be fully consistent with the applicable European legal framework".[79]

Nonetheless, in another hypothesis of fight against copyright infringement, it can be said that IP addresses are *not* used *to identify* websurfers. This was the case in *Ireland*, as regards *EMI Records et al. v. Eircom* (IEHC 2010). It is important to make the point that Justice Charleton, delivering the judgment, was "convinced, on the basis of the affidavit evidence before [him], that the plaintiffs have no interest at all in using this process to find out who the copyright infringers are. Rather, what they are interested in is having the protocol work so that the plague of copyright infringement may be undermined"[80] (emphasis added by author). So, the aim of plaintiffs was not to "directly take action against each such illegal downloader".[81] Therefore in their hands, IP addresses would not be personal data. In *Belgium*, as regards filtering, the Brussels Court of First Instance[82] seems implicitly to have deemed that IP addresses were not personal data. It decided this way in a context involving filtering and blocking software that IAPes could use to prevent peer-to-peer sharing of copyrighted works through their networks. The court considered that this software, like antivirus software, did not amount to activities implying the identification of websurfers.[83] But in both the Irish and the Belgian case, the intended purpose was to have an effect on users' behavior. In the first case, the user faced the risk of a suspension of his Internet access. And in the second one, the relevant data packets could not be communicated through the IAP network. In this respect, such a purpose viz. to obtain a certain ""result" element", "to have an impact on a certain person's rights and interests", has been taken into account by the Working Party 29 in its understanding of the concept of personal data (WP136).[84] In other words, it could be argued that processing of personal data could be at stake in the present cases. And as regards the three strikes procedure, the European Data Protection Supervisor does not hesitate to generally deem that it involves the processing of personal data: "it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data in all cases relevant here."[85]

Finally, beyond the fight against online copyright infringement, IP addresses are clearly at the heart of litigation related to the Internet since they constitute the most effective means to identify an infringer, for example whether it be question of defamation – in *Doe v. Cahill* (Supr. Ct. Delaware 2005)[86] or in *J.F. v. SAS Networks* (TGI Paris 2008) –, of child pornography – in *USA v. Steiger* (11thCir. 2003) –, or of the conviction of a journalist for illegally providing state secrecy – in *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007),[87] etc.

To conclude, often IP addresses are especially processed to sue and to identify websurfers.

4. Arguments against the IP addresses' status of personal data

4.1. *Limitations of the IP address as identifier*

Except where the IAP provides the IP address, no one can, with reasonable means and without any other information, identify the subscriber/user of the address. The IP address only relates to a computer. In *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007),[88] the Hong Kong data protection ordinance was applied.[89] The Appeal Board considered that an IP address is assigned by an ISP "to the user's computer"[90] and that such an address "cannot reveal the exact location of the computer concerned or the identity of the computer user".[91] So it is not "*per se*" personal data. It has to be combined with other

[79] Hustinx PJ. Protection of personal data on-line: the issue of IP addresses; 2009, p. 7, from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15_adresses_IP_EN.pdf [accessed 05.10.10] (also published in *1 Legicom,* 2009, n°42). At the present time, a bill proposes to clarify the status of IP addresses, proposing that they be protected according to the French data protection act, *see* http://www.senat.fr/rap/l09-330/l09-3302.html [accessed 06.10.10].

[80] *EMI Records et al. v. Eircom* (IEHC 2010), no. 12.

[81] *EMI Records et al. v. Eircom* (IEHC 2010), no. 24.

[82] Tribunal de Première Instance de Bruxelles, June 29, 2007, *s.c.r.l. Société belge des auteurs c. s.a. Scarlet*, retrieved on October 4, 2010, from http://www.juriscom.net/documents/tpibruxelles20070629.pdf. An appeal has been filed against this decision, before the Cour d'appel de Bruxelles. The latter sought a preliminary ruling to the ECJ. At the time of finalizing the present paper, the case is pending before the ECJ (Scarlet Extended SA v. Sabam, Case C-70/2010), and the Advocate General Cruz Villalon has already presented his opinion on April 14, 2011. His opinion has however not been analyzed for the purpose of the paper.

[83] The Court underlined that "les logiciels de filtrage et de blocage ne traitent en tant que tels aucune donnée à caractère personnel; […] à l'instar des logiciels antivirus ou antispam, ils sont de simples instruments techniques qui comme tels ne réalisent pas d'activités impliquant l'identification d'internautes" (*s.c.r.l. Société belge des auteurs c. s.a. Scarlet,* TPI Bruxelles, 2009, p. 10).

[84] Article 29 Data Protection Working Party, Opinion n°4/2007 on the concept of personal data, June 20, 2007, hereinafter referred to as "WP136", p. 11.

[85] European Data Protection Supervisor, *op. cit.*, no. 27.

[86] The case was about defamation through blog postings, Supreme Court of the State of Delaware, October 5, 2005, *John Doe no. 1 v. Patrick Cahill and Julia Cahill*, 884 A.2d 451, No. 266, 2005.

[87] Administrative Appeal Board (Hong Kong), November 26, 2007, *Shi Tao v. Privacy Commissioner for Personal Data,* administrative appeal n°16 of 2007, retrieved on October 6, from http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf.

[88] As regards the case, *see* Office of the Privacy Commissioner for Personal Data, *Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's perspective,* Second Edition, Hong Kong, 2010, pp. 13–14, from http://www.pcpd.org.hk/english/publications/files/Perspective_2nd.pdf [accessed 05.10.10].

[89] As regards the definition of personal data, Hong Kong Personal Data (Privacy) Ordinance, Ordinance n° 81 of 1995, section (2) states: "personal data means any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable".

[90] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), nos. 30–31.

[91] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), nos. 30–31.

information.[92] In the same sense, in France,[93] the Paris Court of Appeals decided, in *Anthony G. v. SCPP* (CA Paris 2007), that IP addresses were not personal data because only the legitimate competent authority (the police, and not the collecting society involved in the case) was able to investigate and obtain from the IAP the identity of the subscriber at stake. Another French court underlined, in *Henri S. v. SCPP* (CA Paris 2007), that an IP address related to a computer and not to the individual who used it. In *EMI Records et al. v. Eircom* (IEHC 2010), the High Court of Ireland emphasized, as regards the identity of websurfers, the following: "there seems no legal avenue open to [the majors] to get that information apart from an application for the names and addresses of the copyright thieves to the internet service provider.[94] It is proved to me to be close to impossible that they could have recovered them by any easier or less pricey means".[95] Such a procedure therefore does not seem to constitute a reasonable means to identify websurfers when the collector of IP addresses does not intent to begin such a lawsuit.[96]

However, four nuances have to be offered in respect of the above-mentioned reasoning. These nuances notably show that what is a reasonable means to identify an individual can rapidly expand. Firstly, depending on the *purpose* pursued by the collector of the IP addresses, a judicial procedure can be deemed to constitute a reasonable means to identify a living individual.

Secondly, data in possession – or that could come in the possession – of the collector have to be taken into account. This has to be assessed considering the services offered by the collector and the relevant market at stake. On the one hand, numerous websites record their visitors' IP addresses while, at the same time requiring them (often by contract and through a web form) to identify themselves on the website. This is, for instance, the case in respect of numerous social networking sites such as Facebook.[97] In another example, Google requires its users to give true information about themselves if asked by the registration process of the service at stake (e.g. the well-known Gmail).[98] This means that through their different services – e.g. YouTube and Gmail –, these companies have *the technical capacity to* identify who is the user (subscriber to the IA service or not) behind an IP address.[99] When a company offers a service through which users are identified and their IP addresses are recorded, such company is technically able to identify these users with their IP addresses through any of its services holding the record of IP addresses. This is correct at least as long as the user is logged on to his account.[100] This is all the truer as regards cloud computing technologies when providers offer infrastructure or platforms as services. The IP address could be used to track a logged user. This reasoning is also all the truer when Internet Protocol version 6 [IPv6] addresses are used. Indeed, IPv6 addresses comprise a permanent unique identifier related to the hardware of the user's terminal (derived from the MAC address).[101] This means that all the connections made via the specific terminal of a user will be identifiable and linkable. However, this specific privacy concern could be avoided if the default settings of IPv6 are changed, which seems possible.[102]

On the other hand, such a capacity to link IP addresses to individuals also arises when companies merge in the Internet services market. Corporate merging implies a possible database merging, in any case, the capacity for a same "data controller" to access both databases at once. Famous mergers can be cited: Google acquired DoubleClick and also acquired

[92] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), nos. 30–31.

[93] According to French law, in order to determine if a natural person is identifiable, all the means that enable to realize its identification must be considering including means available to the data controller or to any person, or means that can be accessed by these latter, *see* Article 2 of the Loi n°78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (consolidated version of 30 June 2010), available on http://www.legifrance.gouv.fr.

[94] What Justice Charleton is convinced they do not want to do, *see infra*.

[95] *EMI Records et al. v. Eircom* (IEHC 2010), no. 24.

[96] In Ireland, according to section 1 of the Data Protection Act 1988, personal data are: "Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller".

[97] *See* clause n°4: Registration and Account Security of Facebook terms of use, available on http://www.facebook.com/terms.php?ref=pf [accessed 05.10.10].

[98] *See* clause 5.1 of Google terms of service, available on http://www.google.com/accounts/TOS?hl=en [accessed 05.10.10].

[99] In the United States, it seems that such reasoning would be refuted. *See* US Court of Appeals for the Sixth Circuit, September 28, 2006, Klimas v. Comcast Cable Communications, Inc., 465 F.3d 271, retrieved on October 5, 2010, from http://www.ca6.uscourts.gov/internet/index.htm. It was alleged that the IAP Comcast had recorded the Web traffic of its subscribers (their IP addresses and the URL visited). The relevant rule at stake related to the collection of subscribers' personal data, and was taken from the Cable Act 1984 (45 U.S.C.A. § 551). The Court firstly considered that the Cable Act 1984 did not apply to broadband Internet service (p. 5). The Court underlined that the Cable Act 1984 only defines what was not personal data. Are not personally identifiable information, "any record of aggregate data which does not identify particular person". Then the In this respect the Court considered that "[t]he only record containing the identity of "particular persons" mentioned in the complaint, as noted above, is the list of Comcast internet service subscribers, which – standing alone – obviously is not covered by the Act" (p. 8). It is interesting to note that the Court previously precised that the "complaint also alleged that the defendant had information from which it could identify its subscribers, but not that the defendant had actually correlated the IP–URL linkages with the subscriber list". Therefore it seems that in the Court's view, it is not sufficient that a correlation *may* be done between databases. For personal data to be at stake, a correlation should have been *actually* done.

[100] If the IPv4 address is static, then the identification is also possible when the user is not logged onto the service. The same is true as regards a dynamic IP address when the service provider uses identification cookies. *See infra* as regards IPv6.

[101] See notably http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping.htm; http://www.openwall.com/presentations/IPv6/; http://technet.microsoft.com/en-us/library/cc736439%28WS.10%29.aspx; http://en.wikipedia.org/wiki/MAC_address.

[102] See European Commission IPv6 Task Force, Discussion document from the European Commission IPv6 Task Force to Article 29 Data Protection Working Group, February 17, 2003, available on http://www.ec.ipv6tf.org/PublicDocuments/Article29_v1_2.pdf, pp. 2-3 ; IETF, T. Narten, R. Draves and S. Krishan, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, September 2007, available on http://tools.ietf.org/html/rfc4941.

YouTube. What would happen if Megaupload Limited, operating the well-known megaupload.com file-sharing website, bought Facebook Inc. – or the reverse? Clearly, the databases of both companies pursue different purposes and should legally be maintained separately according to the purpose compatibility principle.[103] However, it would clearly be technically easy to track identified Facebook users' behavior as regards the Megaupload website via their IP addresses. That's the way an *actual risk* exists. As the web market rapidly evolves and can rapidly change (e.g. Google Buzz trying to enter the social network sites market), numerous databases could merge or be accessed by a same entity.

In these cases, it even appears that "[w]ith a complete listing of IP addresses, one can track a person's Internet usage",[104] even without the help of an IAP.

Thirdly, the sharing of data between affiliates has to be taken into consideration. The Berkley study '*KnowPrivacy*' based on the fifty most consulted websites in the United States at the time of the study has shown the importance of such sharing of data. This is usually foreseen in the privacy policies of websites. The study emphasized in this respect that "[b]ased on our experience, it appears that users have no practical way of knowing with whom their data will be shared", notably underlining that "MySpace, one of the most popular social networking sites (especially among younger users), is owned by NewsCorp, which has over 1500 subsidiaries".[105] This clearly increases the possibilities of identification of users without the need of any IAP.

Finally, if personal data is defined *in abstracto*, and not from the viewpoint of the data controller, it could be argued that IAPes' databases constitute themselves a reasonable means to identify the subscribers; at least as long as the link between the subscriber and the IP address at stake is recorded. Theoretically, such a definition appears to be in use in Belgium,[106] where the *travaux préparatoires* of the Belgian law implementing Directive 95/46/EC specify that a piece of information is personal data, in so far as *someone*, with reasonable means, is able to link this piece of information to a living individual.[107]

These considerations implicitly rely on recital 26 of Directive 95/46/EC. And beyond the context of the fight against copyright,[108] the Belgian Privacy Commission has appeared to consider IP addresses as being personal data. The Commission repeated it six times: first in 2000 there was advice,[109] then, in four further advises,[110] and moreover in an explicative notice related to the declaration of processing.[111] The Working Party 29 also already seemed to have such an *in abstracto* understanding of IP addresses as personal data in its WP148 related to search engines[112] and its WP58.[113] This was also the case in the International Working Group on Data Protection in Telecommunications.[114,115] And the Advocate General Cruz Villalon seems to share the same view too.[116]

[103] See Article 6.1 (b) of Directive 95/46. An IP address recorded by Facebook cannot be used to further identify users' behavior on a different website.

[104] Supreme Court of the State of New Jersey, April 21, 2008, *State of New Jersey v. Shirley Reid*, 195N.J. 422, 949 A.2d 850, p. 16, from http://www.jdsupra.com/post/documentViewer.aspx?fid=f4f80aa4-908e-4092-9397-29c23282be59 [accessed 05.10.10].

[105] Berkeley, School of Information, J. Gomez, T. Pinnick and A. Soltani, "KnowPrivacy", June 1st, 2009, p. 28, retrieved on April 10, 2010, from http://knowprivacy.org/. The study continues: "[h]owever, the numbers we compiled do not include subsidiaries of subsidiaries"…

[106] The concept of personal data is defined by Article 1, § 1 of the loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B. 18 mars 1993, available on http://www.ejustice.just.fgov.be/loi/loi.htm.

[107] *See* Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, exposé des motifs, *Doc. parl.*, Sénat, sess. ord. 1997–1998, n°1566/1, p. 12, from http://www.senate.be/www/?MIval=/index_senate&MENUID=10000&LANG=fr [accessed 07.10.09].

[108] *See* footnote no. 68.

[109] After having discussed the role of IP addresses as regards the "profile" of websurfers, the commission considered that, *in any event*, it is possible, with the help of the ISP, to obtain complementary information related to the user (and to find, for instance, his phone number, his name or his address), *see* Commission for the protection of privacy, Avis d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique, n°34/2000, 22 November 2000, pp. 4–5.

[110] *See* Commission for the protection of privacy (Belgium), Avis relatif à l'avant-projet de loi transposant la directive 2003/98 du Parlement européen et du Conseil concernant la réutilisation des informations du secteur public, n°4/2006, 8 February 2006, p. 4, and two other similar advices related to the implementation of Directive 2003/98/EC, avis n°11/2006, 3 May 2006, p. 4, and n°19/2006, 12 July 2006, p. 4.; Commission for the protection of privacy (Belgium), Avis relatif au projet de loi concernant GSM-R, n°5/2006, 1st March 2006, p. 4, footnote no. 4.

[111] Commission for the protection of privacy (Belgium), Notice explicative – déclaration ordinaire, July 2007, p. 21.

[112] Article 29 Data Protection Working Party, Opinion n°1/2008 on data protection issues related to search engines, April 4, 2008, WP148, p. 8: "Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address".

[113] Article 29 Data Protection Working Party, Opinion n°2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, May 30, 2002, WP58, p. 3.

[114] The International Working Group on Data Protection in Telecommunications has globally considered that: "It is now widely recognized that IP address – and *a fortiori* a unique identification number integrated in the address – can be considered as personal data in the sense of the legal framework" (International Working Group on Data Protection in Telecommunications, "Working Paper on the Use of Unique Identifiers in Telecommunication Terminal Equipment: The Example of IPv6", 31st meeting of the International Working Group on Data Protection in Telecommunications on 26–27 March 2002 in Auckland, p. 2).

[115] It also seemed that IP addresses are personal data for all the European privacy commissions ("*L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes*"), *see* http://www.cnil.fr/index.php?id=2244, [accessed 06.03.08]. However for instance, the UK Information Commissioner's Office does not seem to have such a cut view about the topic, *see* footnote no. 150.

[116] Opinion of the Advocate General Cruz Villalon, Case C-70/2010, *op. cit.*, nos. 75–78.

4.2. *IP addresses can be linked to legal entities that are not protected under Directive 95/46/EC*

This applies for instance, in the case of Network Address Translation (NAT) used for a corporate, university and Internet café, etc., networks. In *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), Yahoo! communicated Yahoo! account registration information and traffic data (IP address, date, hour, phone number and even some content data related to emails) to the competent authorities investigating the identity of a journalist. The journalist divulgated information sent by the Chinese government to the newspaper he worked for. The Appeal board concluded that even coupled with these data, the IP address was not personal data. Therefore, Yahoo! had not communicated personal data. Reaching that conclusion, the board stated that "the Verdict does not indicate that the corresponding user information of the IP address belong to the Appellant or reveal the Appellant's identity".[117] It also underlined that "the address of the account holder will be the address of a business, rather than an individual's address".[118] Also, as regards the registration information of the users of Yahoo! email services, "There was no guarantee that the information so provided was genuine as many users did not register with real information".[119] Anyway "the user name of the Email Account registered with yahoo.com.cn was not the name of the Appellant".[120] So the conclusion of the Appeal Board was that: "the Email Address, or the IP address, did not *ex facie* reveal the *identity* of the Appelant. The information provided by Beijing Yahoo! only disclosed that the email was sent from *a computer* located at the *address of a business entity*, and the date and time of the transaction. Short of CCTV evidence, it would not be reasonably practicable from such information *to ascertain* that it was actually the Appellant who used the computer identified by the IP address to send out the relevant email at the material time [(emphasis added by author)]. It could have been anyone, as long as he had access to that computer (or had the necessary password if one was required at all)".[121] The Board is "of the view that although the information provided to the PRC authorities related indirectly to an individual, it was not such as would enable the identity of the Appellant *to be ascertained* directly or indirectly *with reasonable practicability*"[122] (emphasis added by author).

When NAT is used, different users have the same public IP address while they each have their own in the private network (of a business, university, Internet café,[123] familial housing, etc.).[124] In such a hypothesis, two elements have to be discussed as shown by the previous case. On the one hand, it is true that different people can use the computers at stake and that it cannot necessarily be *ascertained* who actually used the computer at any one time. However, clearly, in European data protection law, "[f]or information to be 'personal data', it is not necessary that it be true or proven".[125] In other words, it does not matter to whom the information at stake is related, insofar as it is related to a living individual. On the other hand, when the subscriber to an Internet access service is a legal entity,[126] the public IP address appears not to be linked to a living individual. However, the local network administrator may record the use of the private network by its users (employees, students, members of a family,[127] etc.) and identify them via their login information or even with the Medium Access Control address[128] [MAC address] of their computer, used for network monitoring (security, integrity, etc.) purposes. Since the MAC address is a unique hardware identifier of a computer network card, identification of the user via his computer is then possible if no specific login is required. J.J. McIntyre[129] quotes an interesting American case, *USA v. J.T. Heckenkamp* (9thCir. 2007),[130] where a network administrator identified a student in the network of his university. Usually, while a student connects to the Internet in their university or school, they do it through their personal login that identifies them. But it has to be conceded that if the administrator of the private network does not record what happens over his network, then it remains impossible to identify a particular terminal of the network and the IP address can no more be related to a living individual. Such a case however will most probably be a rare exception, while the use of networks remains monitored as a general rule. Also, network administrators generally know who has which login. Finally, again, the transition to the IPv6 can make the identification of terminals, and therefore of users, easier. Broadcasting a unique identifier derived from the MAC address would imply that the server log files are no longer necessary to identify the used terminal and its user.

[117] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), no. 63.
[118] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), no. 64.
[119] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), no. 64.
[120] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), no. 66.
[121] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), no. 67.
[122] *Shi Tao v. Privacy Commissioner* (AAB Hong Kong 2007), nos. 69–70. It is important to note that the ruling of the Court would have been different if an IAP was at stake, *see* no. 71.
[123] *See infra* footnote no. 131.
[124] Sometimes, computers in a corporate (or other) network have each their own public IP address, which means that NAT is not used. In such cases, what is explained about NAT is all the truer.
[125] WP136, p. 6.
[126] If the subscriber is a living individual, then the public IP address is related to such an individual and can fall in the scope of Directive 95/46/EC.
[127] Admittedly, it is most probably not the case as regards a familial housing. But generally, the subscription to IA service is made by a living individual. The case of private students housings could be more debatable. Indeed, the owner could have created, for instance, a real-estate company. And the subscription to Internet access could have been made by the legal person while there is no traffic monitoring of the use of the connection.
[128] Institute of Electrical and Electronics Engineers IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. IEEE Std 802-2001, pp. 6, 11 and 20–21, from http://standards.ieee.org/getieee802/download/802-2001.pdf [accessed 07.10.10].
[129] McIntyre JJ. The number is me: why internet protocol (IP) addresses should be protected as personally identifiable information. *DePaul Law Review*, no. 60, 2011, forthcoming, retrieved on http://www.ssrn.com.
[130] U.S. Court of Appeals for the Ninth Circuit, *USA v. Jerome T. Heckenkamp*, April 5, 2007, 82 F.3d 1142 (9th Cir. 2007), pp. 3–6, from http://www.ca9.uscourts.gov/datastore/opinions/2007/04/04/0510322.pdf [accessed 06.10.10].

4.3. Unusual uses of the Internet

Less usual uses of Internet include public proxies with NAT servers (other than the cases of NAT abovementioned)[131] and IP spoofing.

"IP Spoofing"[132] refers to a kind of usurpation of someone else's IP address. It appears to be associated with computer attacks as it is for instance used for "Man in the Middle Attacks" (aka "TCP Hijacking")[133] and also "is a frequent tool in distributed denial-of-service (DDoS) attacks and intrusions.[134] Such hypotheses, where computer hacking is at stake, does not seem relevant as regards the qualification of an IP address.

More relevant is the use of a public proxy server, that is to say: "a computer system or router that breaks the connection between sender and receiver".[135] A proxy server relays the request of websurfers. This means that, when surfing the Web, the users of the proxy will appear "undercover" with the public IP address given by the proxy server. And the actual IP address he was allocated from his IAP will only be disclosed to the proxy server. Then, if the proxy is provided by a legal person, the public IP address no more relates to an identifiable living individual. But it can be observed that the proxy server might store the different connections realized by the individual having recourse to his service. He can even store his client information (identity and credit card number) if the proxy service is a service for which the websurfer has to pay. So, with the collaboration of the proxy server provider, the original IP address of the websurfer may be revealed. However, if the proxy server provider never stores his users' traffic data, these latter become, as a rule, no longer identifiable.

4.4. Processing IP addresses within Directive 95/46/EC

To subject the processing of IP addresses to Directive 95/46/EC is too high a cost for the Internet industry. As P.J. Hustinx rightly observed, if IP addresses are considered to be "often" personal data, "the consequence is that large parts of the Internet economy will be subject to data protection safeguards – such as specific obligations for responsible parties and oversight by supervisory authorities – at least in the European Union".[136] This is an economico-political argument that raises concerns the present paper cannot deal with. One can only note some brief considerations. Firstly, IP addresses are already targeted by Article 5.1 of Directive 2002/58/EC[137] so their processing is not completely free. Secondly, not all information society service providers record the IP addresses of their users, nor do they have to do so. For instance, "Ixquick" search engine providers do not record the IP addresses of their users,[138] and it seems that "Torrentspy" website providers do not either.[139] It is possible for website providers not to store "Server Log Data" (notably IP addresses and requests of their users). For instance, Microsoft Internet Information Service 6.0 makes it possible to disable its logging functionality. The requests of users may also be diverted through an intermediary proxy who caches the website at stake and is geographically closer to the users that request a page. This then prevents the website provider from knowing server log data.[140]

In any case, if the processing of IP addresses was technically necessary to provide the service, such processing would normally not be problematic as regards privacy. Even as regards data protection, it would be necessary for the performance of the contract – provision of a service. And thirdly, if general

[131] We separated this case as relevant to the previously discussed hypothesis of NAT for two main reasons. On the one hand, as regards proxies now discussed, there are two public IP addresses: the one of the proxy server and the one given by its IAP to the websurfer. And on the other hand, in the NAT case abovementioned, the user is "affiliated" at least to some extent with the corporate (or individual) that provide him Internet access (a relative in the family housing, his employer who provides the corporate network, the administrator of the Internet café where he connects to the Web, the University where he is a registered student, etc.). In other words, in the present hypothesis, the linkage between an individual and the broadcasted IP address is less probable. Admittedly, the same could be sometimes said about an Internet café (if the owner of the Internet café does not record anything about the use of the computer he rents).

[132] "IP spoofing is the practise of forging various portions of the Internet Protocol (IP)", http://spoofer.csail.mit.edu/faq.php, [accessed 07.10.10].

[133] See Gerphagnon J-O, Portes de Albuquerque M, Portes de Albuquerque M. Sécurité informatique, Attaques informatiques, pp. 7–13, from http://www.rederio.br/downloads/pdf/nt00700.pdf [accessed 07.10.10].

[134] Kissel E, Mirkovic J. Comparative evaluation of spoofing defenses. USC/ISI technical report number ISI-TR-655, January 2009, p. 1, from http://www.isi.edu/~mirkovic/publications/spoofer.pdf [accessed 07.10.10].

[135] PCMAG.com Encyclopedia, http://www.pcmag.com/encyclopedia_term/0,2542,t=proxy+server&i=49892,00.asp, [accessed 07.10.10].

[136] Hustinx PJ. Protection of personal data on-line: the issue of IP addresses, 2009, p. 1, from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15_adresses_IP_EN.pdf [accessed 05.10.10] (also published in *1 Legicom,* 2009, n°42). At the present time, a bill proposes to clarify the status of IP addresses, proposing that they be protected according to the French data protection act, *see* http://www.senat.fr/rap/l09-330/l09-3302.html, [accessed 06.10.10].

[137] *See supra*. In this respect, it could be argued that it is therefore not useful to consider IP addresses as personal data. However, the scope of Article 5 of Directive 2002/58/EC could be disputed. For instance, it could clearly be argued that this Directive only applies *when personal data are processed* (*see* Article 1, §§ 1 and 2, and Article 3, § 1). And that article 5 has no specific scope that could derogate from the general scope of the directive. This could lead to the conclusion that IP addresses, if they are not considered as personal data, would only be protected as traffic data if they are processed with other personal data. Anyway, Article 5 of Directive would not solve all the problems linked to the processing of IP addresses not considered as personal data. While if IP addresses are personal data, they are at least covered by the general data protection regime. For instance, this regime would limit the period of storage of the data. Therefore, implementation difficulties are also avoided.

[138] *See* http://www.ixquick.com/fra/protect-privacy.html [accessed 05.10.10].

[139] *Columbia Pictures et al. v. Justin Bunnell et al.* (C.D. Cal. 2007), p. 7, lines 15–16.

[140] *Columbia Pictures et al. v. Justin Bunnell et al.* (C.D. Cal. 2007), pp. 7–8 and 8–10. Of course, if logs are not stored by the proxy and, if they are, if they are not sent back to the website provider.

data protection obligations are considered to be too strict as regards the processing of IP addresses,[141] the legislator might set up, as the case may be, a lighter regime than the general data protection one. In this respect, the legislator would have to act according to Article 13, §§ 1, (g), and 2, and Article 18, § 2, of Directive 95/46/EC (more specifically, Article 13 §§ 1, (g) and 2) in establishing this specific legal regime.[142] For instance, a service provider processing IP addresses of its subscribers would not have to register his processing, while the national implementation of Article 6 of Directive 95/46/EC would fully apply to this processing.

5. When are IP addresses personal data?

From previous developments, we can infer the following hypotheses where IP addresses *generally* are – or are not – personal data. For European IAPes, according to their data retention duties, IP addresses related to living individuals subscribers are personal data at least for a period of six month and, as a rule, depending on the applicable law to their data retention obligations, for a maximum period of two years. Beyond, data should be suppressed. So, it should no more be possible to link the IP addresses at stake to individuals.

When collecting societies (or more generally, rights owners, law enforcement authorities or private investigators) collect and record IP addresses for the purpose of suing and identifying websurfers, IP addresses are personal data. However, the period of retention of IAPes' logs has to be taken into account. Indeed, two years after the original collection of an IP address and the relevant related data (e.g. the visited website and the time of the connection, the shared folders, etc.), the IAPes should no more be able to identify the subscriber to whom they allocated the address. Therefore, this address and the associated data cease being personal data except where other means of identification are available to the collectors (e.g. the identity of the user, or his pseudonym and a more recent IP address, etc.).

Sometimes, information society services providers (e.g. websites, web 2.0 websites, cloud computing service, etc.) collect and store users' IP addresses and contractually require them simultaneously to identify themselves when they register on the service. In such cases all collected IP addresses linked with the user account are personal data. The same is true as regards IP addresses collected via other provided services, if the user is logged onto his account or if he has a static IP – or an IPv6 – address.[143] Indeed, the reasoning is all the truer when the IP address constitutes a unique and permanent identifier. The same reasoning can also apply, *mutatis mutandis,* in case of companies' merger, or between subsidiaries and parent, when databases of different entities make it possible to link an IP address with the identity of its user otherwise collected.

Things become more complicated when information society service providers collect their users' IP addresses without otherwise requiring any identification. It could be argued that litigation – civil or criminal – constitutes a reasonable means to identify users.[144] This would imply that IP addresses would not only be personal data for (and processed by) the litigant collecting party and the information society service provider *communicating* the IP address, but *from the original collection by this provider*. It should go this way, as long as the relevant IAPes have to maintain the links between their subscribers and the allocated IP addresses and as long as the provider does not limit his processing as explained below.

Indeed and in any case,[145] if the provider strictly limits its processing of IP addresses to the *technical* and *temporary* storage,[146] – or, as the case may be, transmission – required for the provision of the service (including some kind of advertisement),[147] and if there are thus no practical means (e.g. software or a function of software) set up to retrieve these addresses for another purpose, then it is clear that IP addresses should not be processed as personal data.[148] In some respects, just as directive 2002/58/EC specifies that its Article 5.1 "shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality",[149] the sole purpose of the processing then would be strictly limited to the provision of the service, and IP addresses would processed – and stored – for a very limited period of time.

However, in all the hypotheses where we concluded that IP addresses are personal data, the use of NAT (through proxies or through the servers/routers of a legal person's private network) is problematic as it can imply that IP addresses relate to non-identifiable – with reasonable means – living individuals. This hypothesis has been described above. Then, IP addresses can no more be personal data, and the previous general conclusion is jeopardized.

[141] Which could have lead to the case law studied in the present paper.

[142] As regards the idea of subjecting the processing of IP addresses to a specific legal regime, *see for instance,* in the same sense in France, F. Chafiol-Chaumont and A. Bonnier. "L'identification des "pirates du Web" à partir de leurs adresses IP, De la qualification du constat probatoire de l'agent assermenté mandaté par la SACEM au projet de loi "HADOPI". *Revue Lamy Droit de l'Immatériel*, no. 49, 2009, p. 89.

[143] *See* supra as regards IPv6 addresses.

[144] What has already be done by the Working Party 29 (see footnote no. 112), what the Paris Court of Appeals has already refused to do (*Anthony G. v. SCPP* (CA Paris 2007) and *Cyrille S. v. SACEM and SDRM* (CA Paris 2010)). In *EMI Records et al. v. Eircom* (IEHC 2010) the High Court of Ireland equally refused to consider that personal data were at stake as regards the majors because they did not have the intent to sue websurfers (while it nonetheless remained possible).

[145] That is to say notably even when the service provider knows the identity of his users.

[146] E.g. in RAM (Random Access Memory).

[147] E.g. when the IP address is temporary sent to an advertiser for the purpose of delivering an advertisement, on real-time, adapted to the visited webpage and to the geographic location of the websurfer, the IP address being then *no further record* by the advertiser.

[148] If IP addresses are stored for a ten of hours simply to process the request of the users, there is no reasonable mean to identify him. But if the service provider is asked by a competent authority.

[149] Article 5.1, *in fine*, of Directive 2002/58/EC.

The above considerations show that it is difficult – not to say impossible – to draw a general conclusion to qualify IP addresses as *always* either being or not being personal data. Moreover, the quoted case law illustrates how judges have difficulties in qualifying IP addresses. It is true that, most probably, these difficulties arise from the fact that the application of the data protection regime is problematic in the cases at stake and that the judges, in order to settle the litigation in an acceptable way, might have to decide that IP addresses are not personal data, thereby avoiding the unwanted effects of the general data protection regime. However that may be, a "relative" understanding of personal data is helpful because both to conclude either never or always that IP addresses are personal data is misleading. The concept of personal data is, for instance, "relative" in the United Kingdom[150] and in Germany.[151] Such definition of personal data focuses on the concrete hypothesis at stake, looking at the situation of the controller. This means, in a nutshell, that information is personal data if the data controller has other pieces of information that make it possible to identify the data subject. More precisely, to reconcile our *contextual* conclusions, we suggest a *contextual* understanding of personal data, taking into account who collects IP addresses (the suspected "data controller") and who might likely access – or be given access to – these collected data. Therefore, the means available to the potential controller (i.e. the collector of IP addresses and linked data) are taken into account. Working Party 29 has itself written: "[T]he extent to which certain identifiers are sufficient to achieve identification is something *dependent on the context of the particular situation*" (emphasis added by author).[152]

Working Party 29 also wrote: "[U]nless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side".[153] In this statement thus appears a kind of *precautionary principle*. In our view with regard to the hypothesis we identified above where IP addresses are generally considered to be personal data, the collector of IP addresses should be *presumed* to be the data controller. He would bear the burden of demonstrating the contrary if he does not process IP addresses as personal data (e.g. the IP addresses collected relate to a proxy using a NAT server and whose provider does not store log data). On the other hand, as regards the hypothesis where we concluded that IP addresses are generally not personal data, they should be presumed as not comprising personal data, except if the potential data subject demonstrates the contrary.

Finally, if economically, it is considered that it is "too much" for the Internet industry to consider IP addresses as personal data in the above-mentioned cases – with so much money being at stake – Member States are then totally free to adopt exemptions and restrictions to their data protection regimes, as has been suggested. In these circumstances they should then be politically interested in assessing the question.

Jean-Philippe Moiny (*jean-philippe.moiny@fundp.ac.be*) *research fellow F.R.S.-FNRS (National Fund for Scientific Research) Research Centre in Information Technology and Law (CRID), FUNDP Namur, Belgium.*

[150] For instance in the United Kingdom, "the same piece of data may be personal data in one party's hands while it may not be personal data in another party's hands" (Information Commissioner's Office. Data protection technical guidance determining what is personal data. p. 11, from http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf, [accessed 05.10.10]). According to the UK Data Protection Act 1998, Section 1 (1): personal data "means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the *data controller*" (emphasis added by author). *See* Korff D. Country studies, Germany. In: Comparative study on different approaches to new privacy challenges. June 2010, p. 3, from http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A6_united_kingdom.pdf [accessed 05.10.10]. *See* p. 6 as regards IP addresses where the author points out that for the UK Information Commissioner's Office seems to consider that IP addresses are not personal data for websites operators – but for IAPes as long as they retain identification data –, except if "if they are actually used by the operator to collate the data from different visits, i.e. to build up a "profile" of the visitor" (p. 6). *See* also Information Commissioner's Office. Data protection good practice note, collecting personal information using websites, pp. 2–3, from http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf [accessed 05.10.10].

[151] *See* Korff D. Country studies, Germany. In: Comparative study on different approaches to new privacy challenges. May 2010, p. 4, from http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf, [accessed 05.10.10]. The author concludes from this sense of personal data that IP addresses are personal data for IAPes but not for the other ones.

[152] WP136, p. 13.

[153] WP136, p. 17.