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.