IP ADDRESSES SUBJECT TO PERSONAL DATA REGULATION

Eneken Tikk[8]

Abstract

The management of cross-border cyber incidents and conflicts requires extensive and detailed information sharing among governmental agencies and the entities responsible for the often privately owned information infrastructure. The data of interest for the investigation and management of cyber incidents comprises of not only details about the course of action and background of the incidents but also real-time reporting on targets and, most importantly, details of the server logs, which make it possible to differentiate the good traffic from the bad, block hostile IP addresses, and trace the origin of the attacks.

The EU legal framework on data privacy is claimed to create obstacles to processing cyber incident data for the purpose of cooperative cyber defence management. This article examines the applicability of the Data Protection Directive to the processing of IP addresses as part of traffic data and offers ways to overcome legal obstacles in exchanging data regarding cyber incidents.

The article concludes that the current interpretation of the Directive by the European Union data protection stakeholders (Article 29 Working Party and Data Protection Superviser) is contradictory and creates confusion on the national implementation level. The article suggests that more clear understanding of the purposes and nature of processing IP addresses is needed in order to reach meaningful argumentation as to whether such processing is subject to the Directive or not.

1. INTRODUCTION

Systematic data protection in Europe dates to the aftermath of the Second World War and arises from the need to face the threat of people being potentially mistreated

8 Ms. Eneken Tikk is a Scientist and the Head of the Legal Team of the NATO-accredited Cooperative Cyber Defence Centre of Excellence. She was a Research Fellow of GMU CIP and is a PhD student of Tartu University Faculty of Law.

based on an abuse/misuse of personal data available to the state.[9] Nowadays, data protection concerns are touching upon almost all areas of regulation and the recent expansion of cyber threats underlines further the significance of data protection in the context of cyber security as well as cyber incident management. Furthermore, the growing amount of cyber incidents indicate the urgent need to review the data protection framework in order to fight against the growing risk of database infiltrations and loss of sensitive information. Additionally, several groups of stakeholders such as government, industry and individuals are concerned with the topic of data protection while the information technology understanding of data may often differ from the meaning and value of data for marketing and e-commerce perspective where profiling is primarily aimed at satisfying the customer and therefore is very much identity-focused.

As network security has grown from everyone's business into a global concern, and thus requires significant coordination and consultation efforts as a prerequisite of success, the topics of data exchange and data protection are becoming prevalent in policy and legal discussions. In comparison to the first wave of cyber crime regulation in late 90-ies that was driven primarily by commercial interests and resulted in the "mild" law enforcement approach, recent developments in the European Union (EU) legal framework such as the Data Retention Directive and the proposal for the Directive on Attacks Against Information Systems point to a more regulated approach.

Increasing security threats are bound to bring along privacy concerns as solving and investigating cyber incidents may potentially involve processing large quantities of data. Following the latest advancement in the "security vs privacy"

9 In 1939, the German authorities conducted a census to register German Jews and those who were half Jewish with the *Reichssicherheitshauptamt*. While the authorities claimed that personal data, such as religious inclination and nationality, were confidential, a national registry was created on the basis of those data to point out which citizens had a Jewish parent or grandparent. Similar registries were created and updated in Poland and compared to the data of the 1933 census. After the census, the German citizens were listed in the *Reichskartei* as Aryans or non-Aryans and their fate for the purposes of the Second World War was determined by the Nazi authorities controlling those registries. In this context, the statistical data was put to the service of the governing regime. Extremely high regard to population policy transformed normally quantitative data about people into a qualitative and psychological basis of reigning. Although statistical in nature, this information relied on the penetration of private and public lives, recording and categorising such data, and last but not least, subdivision of the data. The census data based on religion and nationality were not the only listed categories of information. In 1935, the authorities created the labour registry, in 1936 the health registry, in 1939 the population registry, and in 1944 the personal identification number system. From 1934 on, those with hereditary illnesses were registered. By the beginning of the war, the authorities had a clear picture of family planning, land inheritance and health status of the population. These statistics were put to service by and under the control of the authorities. Summarized from „The Nazi Census: Identification and Control in the Third Reich (Politics, History, and Social Change)" by Gotz Aly, Karl Heinz Roth, Edwin Black, and Assenka Oksiloff, Temple University Press, 2004.

polemic, the application of data protection rules in responding to cyber incidents needs even further attention from IT security stakeholders since IP addresses and other network traffic data that is daily exchanged between trusted parties around the world may be viewed as personal data and consequently, their processing may be rendered legally problematic.

This article uncovers some of the most challenging issues in the debate on whether IP addresses should be considered as personal data and thereby subject to the EU Data Protection Directive 95/46/EC[10]. Moreover, it needs to be analysed to what extent other EU legal instruments apply to the regulation of IP addresses and what is the Working Party 29 (WP 29) position in the slightly controversial matter.

2. THE PROBLEM AROUND THE INTERPRETATION OF THE DATA PROTECTION DIRECTIVE 95/46/EC

Essentially, the EU data protection regulatory framework is based on the prohibition of processing personal data and has issued different exceptions that allow the data to be processed under a set of personal data protection principles and restrictions.

Directive 95/46/EC has become the cornerstone of data protection in Europe and serves as the basis and a role model for personal data protection legal acts in more than 30 advanced information societies worldwide. Currently, personal data can be freely exchanged and processed between the 27 EU member states and three European Economic Area (EEA) member countries (Norway, Liechtenstein and Iceland) and to Switzerland, Canada, Argentina, Guernsey, and the Isle of Man. Transfer of personal data to the third countries is only allowed if the third country in question ensures an adequate level of protection.[11] An exception to that principle is granted to the US Department of Commerce under the Safe Harbour Framework[12], and the transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection[13]. Not surprisingly, one of the most critical problems includes the legal difficulties in exchanging data between nations, authorities, industry and other stakeholders.

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, available online at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

11 Data Protection Directive 95/46/EC, Chapter IV, Transfer of data to third countries.

12 *US-EU & Swiss Safe Harbor Frameworks, available online at: http://www.export.gov/safeharbor/.*

13 Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security, DHS, 2007 PNR Agreement.

In the context of sharing cyber incident data, one possible interpretation of the Directive leads to the conclusion that collecting and exchanging IP addresses is subject to the conditions provided for in the Directive. The other leaves IP addresses out of the immediate scope of the applicability and requires the Directive to be followed only in case the use of IP addresses would identify the person behind it. Hence, the essence of the problem lies in determining the scope and ability of IP addresses to perform as individual identifiers as well as the applicability of the EU Data Protection Directive.

The first elements of the puzzle are inevitably the definitions of "IP addresses" and "personal data". Electronic Privacy Information Centre's (EPIC) approach to describing an IP address as part of traffic data is generally widely supported:

> "A device's (typically a computer's) numerical address as expressed in the format specified in the Internet Protocol. In IPv4, the current addressing format, an IP address is a 32-bit sequence divided into four groups of decimal numbers separated by periods. In some circumstances, the IP address identifies a unique computer. In other circumstances, such as when a network of computers connects to the Internet via a single Internet connection, it may not. An IP address for a computer is similar to a telephone number for a telephone."[14]

As the foundation for the forthcoming discussion the article employs the terminology of the EU Data Protection Directive whilst it is useful to note that not everyone involved in the debate is proficient in and uses the terminology of the Directive. When engaging in discussions with the US legal communities, the term "personally identifiable information" (PII) comes up, which essentially is a synonym to "personal data" as defined in the Directive.

The Directive defines as personal data and therefore as potentially applicable to processing "any information relating to an identified or identifiable natural person ("data subject")".[15] 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[16].

Further, the word "indirectly" plays an important role in how this definition is understood in the context of IP addresses. The Directive itself provides no further definition for this term, but it has been addressed by Article 29 Working Party[17] set up under Article 29 of the Data Protection Directive.

14 Definition of an IP address, Electronic Privacy Information Centre, available at: http://www.epic.org.
15 Article 2 (a) of the Directive.
16 Article 2 (a) of the Directive.
17 WP 29 is an independent European advisory body on data protection and privacy having great influence on national interpretation of the Directive.

According to WP 29, as regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others.[18]

Although not the core of this debate, another important term is "processing" that for the purposes of the applicability of the Directive means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[19] Thus, if concluded that IP addresses are personal data, the Directive is applicable to all possible occasions of processing.

Therefore it is of utmost importance to reach a conclusion whether IP addresses should be considered as personal data. Should that be the case, several entities such as Internet Service Providers (ISPs), search engines, etc would be subject to a number of obligations stated in the Directive. For example, the data controller (the entity processing data) is responsible for ensuring that data be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, accurate and up to date as well as kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[20] Most importantly, the controller is obliged to provide information about the fact of the processing as well as the existing data to the data subject.[21]

3. APPLICABILITY OF THE DATA PROTECTION DIRECTIVE TO THE PROCESSING OF IP ADDRESSES: VIEWS AND REASONING

Needless to say, there are several contradicting opinions about the applicability of

18 Opinion 4/2007 on the concept of personal data (WP 136). Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.
19 Article 2 (b) of the Data Protection Directive.
20 Data Protection Directive 95/46/EC, Article 6.
21 Data Protection Directive 95/46/EC, Article 6.

the Directive.[22] The views on the debate concerning IP addresses that have been echoed by the EU Data Protection Supervisor (EDPS), Working Party 29 and several data commissioners[23] are rather conservative, in most cases regarding IP addresses and traffic data as personal. This chapter will look into the recent policy discussions in the EU, opinions of Article 29 Working Party (hereinafter WP 29), an independent EU Advisory Body on Data Protection and Privacy established by Article 29 of the Data Protection Directive, and introduce two further directives impacting the processing of IP addresses.

3.1 Position of the European Union Data Protection Supervisor

According to the European Union Data Protection Supervisor (EDPS) Peter Hustinx, a person does not have to be identifiable by name for data protection law to apply to details of their computer usage. Hustinx stated that companies, if in doubt, should treat all user activity, server logs and records of IP addresses as personal data. The Data Protection Supervisor further claimed that in order for an IP address to count as personal data there is no requirement for the company processing the data to know details such as the name, birth date or other personal data of the individual whose activity it was monitoring. Rather individuals are identifiable when they are singled out and, according to Hustinx, tracking the behaviour of individuals by their IP address singles individuals out in such a way as to make them identifiable.[24]

In a recent opinion on the current negotiations by the European Union on the Anti-Counterfeiting Trade Agreement (ACTA) the EDPS[25] has once again underlined the importance of the regulation of personal data processing. Even though the opinion is determined to focus on intellectual property infringement, it clearly scrutinises the relationship between IP addresses and personal data.

In the above-mentioned opinion the EDPS notes that Directive 95/46/EC is applicable to the processing of IP addresses involved in the three strikes Internet disconnection policies where the IP addresses "should be considered as personal

22 Article 29 WP Asks More Data Protection From Search Engine Operators, Digital Civil Rights in Europe, available at: http://www.edri.org/edrigram/number8.11/article-29-wp-search-engines; Working Party 29 Chairman Jacob Kohnstamm's letter to Google, 26 May 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf.

23 Aoife White, IP Addresses Are Personal Data, E.U. Regulator Says January 22, 2008, available at http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html.

24 *Via McCann FitzGerald Solicitors;* ZDNet interview with Peter Hustinx, available at: http://news.zdnet.co.uk/security/0,1000000189,39540137,00.htm.

25 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010/C 147/01, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf.

data. IP addresses are identifiers which look like a string of numbers separated by dots, such as 122.41.123.45. A subscription to an Internet access provider will give the subscriber access to the Internet. Every time the subscriber wishes to go onto the Internet, he will be attributed an IP address through the device he is using to access the Internet (a computer, for example)".[26] Hereby EDPS confirms its earlier position that IP addresses should be viewed as personal data.

EDPS continues that "the principles of protection must apply to any information concerning an identified or identifiable person" and confirms that if a user engages in a given activity, for example, uploads material onto the Internet, the user may be identified by third parties through the IP address he/she used.[27] Therefore, for the purposes of ACTA:

> "Traffic data such as IP addresses may only be collected and stored for reasons directly related to the communication itself, including billing, traffic management and fraud prevention purposes. Afterwards, the data must be erased. This is without prejudice to the obligations under the Data Retention Directive which, as discussed, requires the conservation of traffic data and its release to police and prosecutors to aid in the investigation of a serious crime only. This means that, when contacted by copyright holders, unless such contact occurred within the limited period outlined above, ISPs should not have the log files linking the IP addresses to the relevant subscribers. Retaining the log files beyond such period should only be done for justified reasons within the scope of the purposes provided by law."[28]

3.2 WP 29 opinions regarding IP addresses as personal data

WP 29 opinions are authoritative for the national implementation of the Directive as the body is composed of heads and high-level representatives of national data protection agencies. The advisory body has issued a number of opinions where the topic of IP addresses has been addressed. As will be shown below, the opinions leave very little opportunity for monitoring traffic without being obliged to implement data protection requirements.

WP 29 shares EDPS's perspective on the processing of personal data. WP 29's argumentation in this opinion is reflected already in 2000, where WP 29 considered IP addresses as data relating to an identifiable person. It has stated that "Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally

26 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), p. 25.
27 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), p. 26.
28 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), p. 57-59.

systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive …)."[29]

In its 2008 opinion on search engines, WP 29 observed:

> "A search engine provider that processes user data including IP addresses and/or persistent cookies containing a unique identifier falls within the material scope of the definition of the controller, since he effectively determines the purposes and means of the processing."[30]

WP 29 further explained that in the role as service providers to the users, search engines are collecting and processing vast amounts of user data, including data gathered by technical means, such as cookies.[31] A search engine provider may link different requests and search sessions originating from a single IP address[32]. It is thus possible to track and correlate all the web searches originating from a single IP address, if these searches are logged. Identification can be improved, when the IP address is correlated with a user unique ID cookie distributed by the search engine provider, since this cookie will not change when the IP address is modified.[33] In the context of this article the term "search engine provider" could be compared to an Internet Service Provider.

But even if we were talking about entities monitoring traffic for their own "internal" purposes the opinion of WP 29 would still render them subject to data processing regulation. WP 29's further reasoning concludes that though IP addresses are in most cases not directly identifiable by search engines, identification can be achieved by a third party. Law enforcement and national security authorities can gain access to such 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.[34]

To further explain the effect of this interpretation, these conclusions have impact

29 WP 29 Working Document "Privacy on the Internet - An integrated EU Approach to On-line Data Protection. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.
30 WP 29 opinion on data protection issues related to search engines, 4 April 2008, available at: http://www.registratiekamer.nl/downloads_int/c.1.a_ts_search_engines_adopted_version.pdf.
31 Opinion 1/2008 page 4.
32 An increasing number of ISPs distribute fixed IP addresses to individual users.
33 Opinion 1/2008 page 7.
34 Opinion 1/2008 page 8.

also beyond the EU. According to the SWIFT Opinion from 2006[35] a data controller may effectively be an entity not located on the territory of any EU Member States.

All in all, these arguments create an intriguing "data protection limbo", where data is regarded personal, because it can potentially be accessed by law enforcement and national security agencies, while other directives[36] request the same data to be made available to such authorities.

3.3 Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)

The analysis of the Data Protection Directive is incomplete without regard to the interpretation of Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)[37] adopted in 2002 regulating privacy and personal data protection in the electronic communications sector. This directive introduces the term "traffic data" meaning any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.[38] Although it is important to note that the e-Privacy Directive distinguishes a portion of data for the "communication conveyance" point of view, the aim of the instrument is to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy.[39]

Despite the fact that the Directive does not explicitly address IP addresses, they are still included in the definition of traffic data. The e-Privacy refers to traffic data as a set of data undergoing a different regulatory regime for network conveyance purposes and thereby recognizes to an extent the need to adjust technical and legal notions of data. Yet, the Directive seeks to find a balance and thus stresses that privacy rights remain the primary concern for communication service providers when processing traffic data.

Valuable insights to the current interpretation of the extent of the applicability of the Data Protection Directive to data processing for information security purposes

35 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.
36 E.g. Data Retention Directive.
37 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). Official Journal L 201, 31/07/2002 P. 0037 – 0047. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.
38 Article 2 (b) of the e-Privacy Directive.
39 Article 1 (a) of the e-Privacy Directive.

are provided by WP 29 in an opinion regarding the proposed amendment[40] of the e-Privacy Directive in 2009.[41]

According to the proposed amendments, the public communications providers are obliged to to inform national regulatory authorities of any data security breach. In the process of discussing the amendments, the Parliament proposed to introduce a new Recital (27a) on IP addresses in the e-Privacy Directive.[42] The proposal reads as follows:

"IP addresses are essential to the working of the internet. They are unique numbers assigned to devices participating in a computer network using the Internet Protocol for communication between its nodes, such as computers or mobile smart phones. In practice, they may also be used to identify the user of a given device. Considering the different scenarios in which IP addresses are used, and the related technologies, which are rapidly evolving (including the deployment of IPv6), questions have arisen about their treatment as personal data in certain circumstances. Developments concerning the use of IP addresses should be followed closely, taking into consideration the work already done by, among others, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, and in the light of such proposals as may be appropriate."[43]

The response of the WP 29 to this proposal allows concluding that it considers the issue of IP addresses having been addressed and solved with sufficient clarity:

> "The Working Party does not support the proposal to make an explicit reference to this issue in a directive. In this respect, it re-emphasizes its earlier Opinion[44] that unless the 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

40 New e-Privacy Directive 2009/136/EC that is amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

41 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf.

42 COM (2008) 723 (Amended proposal for Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation (Text with EEA relevance), page 21 (amendment 185). Available online at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0723:FIN:EN:PDF.

43 COM (2008) 723, page 21.

44 Opinion 4/2007 on the concept of personal data and Opinion 1/2008 on data protection issues related to search engines.

personal data, to be on the safe side".

In the above mentioned opinion the Article 29 Data Protection Working Party concludes that unless the 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". IP addresses relate to identifiable persons in most cases. Identifiability means identifiable by the access provider or by other means, with the help of additional identifiers such as cookies or in interactions with internet services with which the data subject is identified explicitly or implicitly.[45]

WP 29 underlines that a substantive provision of a directive is not the most suitable way of addressing this issue and that a reporting obligation referring to "purposes not covered by this Directive" is not appropriate.[46] This remark by the WP 29 puts special emphasis on the service provider's ability to distinguish between the data that can be linked with a certain identity and the data that cannot be identified.

In sum the Working Party has rejected the need to amend the Directive in order to allow processing IP addresses as it sees that this option already exists under the current wording of the Directive. Considering, however, the opinions given under the Personal Data Protection Directive, the two views are opposing. To illustrate this conflict, the Data Retention Directive needs to be looked into.

3.4 Data Retention Directive 2006/24/EC

The Data Retention Directive[47] creates the "missing" link between the data in the communication service provider's possession and the potential processing for law enforcement purposes.

The purpose of the Data Retention Directive is to harmonize Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communication networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data is available for the purpose of the investigation,

45 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf.

46 *Ibid.*

47 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. Official Journal L 105, 13/04/2006 P. 0054 – 0063. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML.

detection and prosecution of serious crime, as defined by each Member State in its national law.[48]

For the purposes of the Data Retention Directive, data means traffic data, location data and the related data necessary to identify the subscriber or the user.[49] IP addresses are data needed to identify a particular user and fall under the categories of data that need to be retained according to Article 5 of the Directive. The data should be retained to the extent that it is generated or processed by providers of publicly available electronic communication services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.[50]

It therefore provides the ground for data exchange between communication service providers and law enforcement. Although defining the exact scope of law enforcement authority is left to national law, the wording of the WP 29 in its Opinion 1/2008 leaves little room for alternative interpretation: if it is likely that the data retained by the communication service providers is available to national authorities upon request, the data is to be regarded as potentially identifying a data subject[51].

4. SUMMARY AND THE NEED FOR FURTHER CLARIFICATION

If we combine the requirements set in the directives with the opinions of the WP 29 and EDPS, we reach a situation where the notion of personal data and therefore the legal implications put forward in the Data Protection Directive are applicable to a very broad range of information. In keeping with these arguments, it appears that the sole option for processing traffic data, including the IP addresses, without falling under the scope of the Data Protection Directive would be during real-time monitoring when no data is stored for further analysis (and availability).

The issue of IP addresses as personal data has also been looked into on the national level. The outcome indicates that countries have taken different positions as regards the implementation of the Directive, which, in the longer run could lead to additional policy concerns in the EU. Positions of national authorities in Germany, France, UK and Sweden illustrate the wide spectrum of approaches[52] where it

48 Article 1 of the Data retention Directive.
49 Article 2 (a) of the Data Retention Directive.
50 Article 3 (1) of the Data Retention Directive.
51 Opinion 1/2008 page 8.
52 The developments in these countries have been covered in more detail in: Tikk, Eneken, Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective. In NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Volume 59, 2009 „Modelling Cyber Security: Approaches, Methodology, Strategies", pages 189 - 198.

becomes evident that, for example, depending on the national regulation and court's interpretation, the dynamic IP addresses may be considered as personal data[53] or as not personal data.[54]

Seen from the EU perspective, difference in opinions poses a threat to the uniform application of the directives and in the broader perspective to the value and position of the EU law in general.

5. RECOMMENDATIONS FOR NATIONAL IMPLEMENTATION

5.1 National Security Exceptions

The applicability of the Directive is bound to its scope. In accordance with Article 3(2) of the Data Protection Directive it shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law /…/ and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

Similarly, Article 15(1) of E-Privacy Directive sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in this Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications systems.

Another perspective that will potentially play a role in the debate around the applicability of the Directive to processing traffic data is processing network monitoring information for law enforcement and national security purposes.[55]

53 District and Regional Court of Berlin, 2006, see more Lundevall-Unger, Patrick, Tranvik, Tommy, IP Addresses – Just a Number?, International Journal of Law and Information Technology, University Press 2010.

54 District court of Munich, 2008, see more Lundevall-Unger, Patrick, Tranvik, Tommy, IP Addresses – Just a Number?, International Journal of Law and Information Technology, University Press 2010.

55 WP 29 has observed that: „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. (Opinion 1/2008 on search engines).

Nations could make use of the national security exception of the Data Protection Directive. The general national security exception should also be included in other legislative instruments, primarily in relation to the authorities and procedures involved.

5.2 Complying with WP29 Opinions

WP 29 has concluded that as long as the service provider in the capacity of data controller is able to distinguish that network traffic data is not personally identifiable, such data is not regarded personal in the context of the EU Data Protection Directive. It would be safe to conclude that real-time monitoring with no data retention would be in compliance with the current regulatory framework of the EU.

Until no further guidance is provided, these are the steps that could be taken by communication providers and national legislative authorities to reduce the risk of processing IP addresses in violation of the Data Protection Directive.

5.3 Following up the discussions on national level

National data protection authorities could serve as the balancing power between cyber security concerns and privacy rights. A balanced guidance on network monitoring would assist communication providers who eventually need to assess the need for network monitoring and make sure that all data processed is proportionate with the actual security assessment and that data is retained for no longer than necessary.

WP 29 concludes that the legislative measures limiting the right to privacy of individuals have to be accessible and foreseeable as regards their implications for the persons concerned.[56] This principle requires the legislation to be sufficiently clear in its definitions of the circumstances, the scope and the modalities of the exercise of interference measures. The provisions have to be unambiguous and go into detail to indicate under which circumstances the public authority authorized to take measures limiting fundamental rights. They should in particular specify where such measures may be used and should exclude all general or exploratory surveillance and offer protection against arbitrary attacks from public authorities.[57]

56 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf.
57 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf.

My personal position is that the decisive factor should not be the nature of IP addresses as such, but the purpose of processing - i.e. IP addresses can be personal data when used in investigation, but for the purpose of managing the networks and possibly also monitoring traffic and exchanging information about anomalies, the important factor is that the purpose of such processing is not to identify the individual (which is the core concern of the Directive) but detecting threats, vulnerabilities and potential defences.

Therefore, for the purposes of law enforcement and also in cases where one would use IP-addresses and other traffic data to identify the person behind an intrusion such data processing is subject to the Directive, but all uses of the same data for network management purposes is not.

5.4 Additional clarification by WP29

So far WP29 has rejected the proposal to clarify the legal framework of processing IP addresses (see section 3.3. "Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)").

Considering the opinions of WP 29 in assembly, an indubious position cannot be derived. It would be therefore rational for the WP 29 to expressly address the issue of processing IP addresses and/or traffic data for the purposes of network security and global cyber security concerns.

Thereby WP 29 would not only respond to an important concern shared by many nations but also eliminate part of the margin of interpretation potentially undermining the value and weight of the EU data protection directives. The guidance given by WP 29 would significantly aid to more coherent implementation of the legal framework of personal data processing by Internet Service Providers, Critical Information Infrastructure entities, law enforcement and those facing cyber attacks as part of their cyber threat assessment.

CONCLUSION

There is no doubt about the interrelation of data protection and cyber security. However, the current definition of personal data appears to restrict monitoring of traffic and detecting anomalies. In addition to the debates in legal and technical communities, the issue of IP addresses has been discussed by a number of national authorities and the results of these discussions reflect a divide of implementation practices. WP 29 has concluded that as long as the service provider in the capacity of data controller is able to distinguish that network traffic data is not personally

identifiable, such data is not regarded personal in the context of the EU Data Protection Directive, but WP 29-s other opinions restrict this position and lead to the conclusion that only real-time monitoring with not data retention is legally feasible. This does not, in many cases, satisfy the needs and requirements of technical experts.

To resolve the issue, difference should be made between processing data for mere monitoring, and processing data in order to identify the IP address user. Also, nations need to make better practical use of the national security exceptions under the Data Protection and E-Privacy Directives.

In sum, a more nuanced approach is needed to whether and under what circumstances IP addresses and other traffic data are to be processed in full compliance with the personal data protection requirements. Also, it should be considered if there are options for partial applicability of the Directives. For a better way ahead, national practices of implementing the Directive need to be studied and analyzed.