10750/02/EN/Final
WP 58

Opinion 2/2002
on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6

Adopted on 30 May 2002

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

has adopted the present Opinion:

The Commission Communication on IPv6

On 21 February 2002, the European Commission adopted a communication to the Council and the European Parliament, focusing on the next generation Internet and the priorities for action in migrating to the new Internet protocol IPv6. This communication takes place in the context of the current development of network services and terminal communication equipment enabled to connect to the network.

The new Internet protocol has been elaborated with a view to facilitate and harmonise the possibilities of connection to the network using multiple terminal equipment, such as mobile phones, personal computers or personal digital assistants, using wireless or cable facilities.

While these developments can only be encouraged, the Working Party would like to stress the need for a careful and in-depth study of the implications of the new protocol in terms of protection of personal data.

The Working Party welcomes the position taken by the Commission in its communication, according to which privacy issues are to be considered in the further development of the Internet. The Working Party stresses, however, that privacy issues raised by the development of the new protocol IPv6 have not been solved yet.

In particular, the possibility of the integration of an unique identification number in the IP address as designed according to the new protocol raises specific concern. In this respect, the Working party regrets that it has not been consulted prior to the adoption of the communication and it expresses the wish to be involved in the coming works taking place on IPv6 at European level.

Data Protection aspects related to the use of unique identifiers in telecommunication terminal equipment

The Working Party takes note of the fact that the International Working Group on data protection in telecommunications has recently issued a working paper on the question of the use of unique identifiers in telecommunication terminal equipment, and it would like to thank the Working group for the work achieved on that subject.

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

The Working Party endorses the conclusions of the working paper adopted in Auckland on 27 March 2002[2], and would like to support its findings by recalling in particular the application of several principles explicitly mentioned in EU directive 95/46 concerning the protection of personal data and the free movement of such data, and EU Directive 97/66 concerning the protection of personal data in the telecommunication sector[3].

The Working Party wishes to emphasise that IP addresses attributed to Internet users are personal data[4] and are protected by EU Directives 95/46 and 97/66.

With reference to the work already achieved with regard to the protection of personal data on the Internet[5], the Working Party would like to stress specifically the following points:

- The unique identifier of an interface, such as the one that might be integrated in IPv6, would constitute an identifier of general application and its use is regulated as such in the legislation of the member States of the EU.

- The principle of proportionality implies that, making a balance between the fundamental rights of data subjects and the interests of different actors involved in the transmission of telecommunication data (such as companies, telecommunication access providers), as few personal data as possible have to be processed.

  This principle has implications on the one hand on the design of the new communication protocols and devices, and on the other hand on the content of national policies related to the processing of telecommunication data: while technology is *per se* neutral, applications and design of new telecommunication devices should be privacy compliant by default. Besides, it should be avoided to generalise measures forcing the systematic identifiable character of telecommunication data.

In that perspective, in the framework of a telecommunication connection, network and access providers should offer to any user the option to use the network or to access the services anonymously or using a pseudonym.

---

[2] See the annex to this document.

[3] Directive 97/66 is being amended in order to take into account technological developments. The provisions of the new directive are intended to protect users of publicly available electronic communications services, regardless of the technologies used.

[4] As recital 26 of Directive 95/46 specifies, data are qualified as personal data as soon as a link can be established with the identity of the data subject (in this case, the user of the IP address) by the controller or any person using reasonable means. In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means.

[5]

§ Working document: Processing of Personal Data on the Internet, adopted by the Working Party on 23 February 1999, WP 16, 5013/99/EN/final;

§ Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, adopted by the Working Party on 23 February 1999, 5093/98/EN/final, WP 17;

§ Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications, adopted on 3 May 1999, 5005/99/final, WP 18;

§ Recommendation 3/99 on the preservation of traffic data by *Internet Service Provide*rs for law enforcement purposes, adopted on 7 September 1999, 5085/99/EN/final, WP 25;

§ Opinion 1/2000 on certain data protection aspects of electronic commerce, Presented by the Internet Task Force, adopted on 3 February 2000, 5007/00/EN/final, WP 28;

§ Opinion 2/2000 concerning the general review of the telecommunications legal framework, presented by the Internet Task Force, adopted on 3 February 2000, WP 29, 5009/00/EN/final;

§ Opinion 7/2000 on the European Commission Proposal for a directive of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector of 12 July 2000 COM (2000) 385, adopted on 2 November 2000, WP 36.

EC Directive 97/66 provides for the possibility for any user to restrict the identification of calling and connected addresses. In Internet communications, anonymity could be reached using solutions such as regularly changing IP addresses used by an individual[6].

- Considering the risks of manipulation and fraudulent use of a unique identifier, the working party recalls that protection measures are needed, taking into account in particular that telecommunication providers are responsible for the security of services they offer. In the framework of the European Union legislation, access providers are obliged to inform subscribers of residual security risks.

- The requirements for privacy compliant default settings in communication devices and for privacy compliance of telecommunication services have been implemented at European level through specific obligations lying mainly on producers of telecommunications equipment, and on telecommunication operators and service providers[7].

Conclusion

The working group strongly encourages research initiatives having as purpose the elaboration of technical solutions to protect the privacy of telecommunication data.

The Working Party is aware that initiatives have already been taken in different working groups in order to find technical solutions to some identified privacy risks, and it considers it necessary to enter into a dialogue in particular with representatives of these groups, and in particular, the Internet Engineering Task Force and the IPv6 Task Force.

The Working Party reserves the possibility to take further steps while evaluating the new design of communication protocols, products and services and while continuing dialogue with actors involved in the design of these new communication tools.

---

[6] Such solution has already been adopted by some access providers, who change approximately every two days the IP address of their ADSL clients.
The implementation of some terminal equipment already takes into account the orientations of RFC 3041 of the Internet Engineering Task Force (IETF), "privacy extensions for stateless address autoconfiguration in Ipv6", January 2001: the terminal equipment uses two types of addresses : an address is generated based on the unique MAC address, and is used for entering communications (e.g. the terminal is always reachable using that permanent address), and another address generated on a (pseudo) random basis, to be used at the initiative of the terminal for outgoing connections.
Thus, when the terminal (and the user behind) is responsible for the connection, it could not be identified through its MAC address.

[7] See Directive 97/66 on the protection of privacy in the telecommunications sector, and Directive 99/5 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal L 091, 07/04/1999.

Annex

Working paper on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6

31st meeting of the International Working Group on Data Protection in Telecommunications on 26-27 March 2002 in Auckland (New Zealand)

Due to a forseeable shortage in the protocol used today for most of the Internet connections (IP version 4), a change of design in the protocol has been elaborated by the international Internet Engineering Task Force (IETF). This new protocol, IPv6, uses a string of 128 bits instead of 32 bits in the former version, to constitute each individual IP address on the Internet.

This new address, thanks to its enlarged capacities, presents many advantages and enables new facilities such as multicasting (quicker transmission of large amounts of data to multiple recipients, e.g. video on-line), voice over IP, etc.

However, the new protocol also raises concerns, as it has been designed in such a way that each IP address can be partly constituted of a unique serie of numbers like a global unique identifier. The introduction of IPv6 might lead to increased risks of profiling of user activities on the Internet[8].

The following preliminary considerations identify the risks and recall the privacy principles to take into consideration while using a unique identifier in the constitution of IP addresses.

I. Identified risks

The characteristics of IPv6 lead to the identification of specific privacy risks, which will depend on the configuration of the new protocol.

- *Profiling issues* are at stake if a unique identifier (the interface identifier e.g. based on the unique MAC address of the ethernet card) is integrated in the IP address of each electronic communication device of the user. In such case, all communications of the user can be linked together, much easier than using cookies as they exist today.

- ***security and confidentiality issues*** **can be identified. These risks are linked with the development of network services, which implies multiplication of the type of terminals connected to the network using the same communication protocol: mobile phones, personal computers, electronic agents controlling home devices (heating, light, alarms, etc.).**

  The new IPv6 protocol allows stable connections, with maintenance of the same address, even when a terminal is moving on the network. Security and

[8] Overall profiling of activities of a user might even be feasible when the same terminal equipment is used in different networks.

confidentiality aspects are at stake here, as there is a risk of identification of location data of this mobile node[9].

II. Data protection principles applicable to IPv6

The working group deems it necessary to draw the attention of all the actors responsible in the elaboration and the implementation of the new protocol, about the national and international legal requirements governing privacy and security of telecommunications.

It is now widely recognised 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[10].

In line with his previous work and the common positions already adopted on that subject[11], the Working Group recalls the following principles, which should be taken into account while implementing the new Internet protocol.

Telecommunications infrastructure and technical devices have to be designed in a way that either no personal data at all or as few personal data as technically possible are used to run networks and services. The unique identifier of an interface as integrated in IPv6 would constitute an identifier of general application.

§ In contradiction with the principle of data minimisation, such use of a unique identifier constitutes a risk of profiling of individuals for all their activities in connection with a network.

§ The protection of the fundamental right to privacy against such risk of profiling must prevail while analysing the different aspects of the new protocol, such as its facility of management.

§ Traffic data, and in particular location data, deserve a specific protection considering their sensitive character[12].
If location information has to be generated in the framework of the use of mobile devices and other objects connected via IP, such information must be protected against unlawful interception and misuse. It should also be avoided that the location information (and the changing in this location information depending on the

---

[9] See e.g. A. Escudero Pascual, "Anonymous and untraceable communications: location privacy in mobile iternetworking", 16 May 2001; "Location privacy in Ipv6 – Tracking the binding updates", 31 August 2001; http://www.it.kth.se/~aep/

[10] See e.g. at European level, the Communication of the Commission on the Organisation and Management of the Internet Domain Name System of April 2000, and the documents adopted by the Art. 29 Data Protection Working Party, in particular "Privacy on the Internet - An integrated EU Approach to On-line Data Protection", WP 37, 21 November 2000.

[11] Common Position regarding Online Profiles on the Internet, adopted at the 27th meeting of the Working Group on 4/5 May 2000;
§ Common Position on Privacy and location information in mobile communications services, adopted at the 29th meeting of the Working Group on 15/16 February 2001;
§ Ten Commandments to protect Privacy in the Internet World
Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements, adopted at the 28th meeting of the Working Group on 13/14 September 2000.
http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm

[12] See the Common Position on Privacy and location information in mobile communications services, adopted at the 29th meeting of the Working Group on 15/16 February 2001.

.

movement of the mobile user), is transmitted non-encrypted to the recipient of the information via the header of the IP address used.

Protocols, products and services should be designed to offer choices for permanent or volatile addresses. The default settings should be on a high level of privacy protection.

Since these protocols, products and services are continuously evolving, the Working Group will have to monitor closely the developments and to call for specific regulation if necessary.

Done at Brussels, 30 May 2002

For the Working Party

The Chairman

Stefano RODOTA