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 (New Zealand)*

Due to a foreseeable 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[1].

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 series of numbers like a global unique identifier. The introduction of IPv6 might lead to increased risks of profiling of user activities on the Internet.

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.).

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

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The new Ipv6 protocol allows stable connections, with maintenance of the same address, even when a terminal is moving on the network. Security and confidentiality aspects are at stake here, as there is a risk of identification of location data of this mobile node[2].

**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[3].

In line with its previous work and the common positions already adopted on that subject[4], 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[5][5].

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 mis-

---

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

[3] See e.g. at the 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; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf .

[4] Common Position regarding Online Profiles on the Internet, adopted at the 27th meeting of the Working Group on 4/5 May 2000 http://www.datenschutz-berlin.de/attachments/188/pr_en.pdf ; 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 http://www.datenschutz-berlin.de/attachments/214/locat_en.pdf ;
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/attachments/216/tc_en.pdf .

[5] 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 http://www.datenschutz-berlin.de/attachments/214/locat_en.pdf .

use. It should also be avoided that the location information (and the changing in this location information depending on the 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.