RESOLUTION

THE USE OF UNIQUE IDENTIFIERS IN THE DEPLOYMENT OF INTERNET PROTOCOL VERSION 6 (IPV6)

November 1, 2011

Mexico City

Sponsor:

Federal Commissioner for Data Protection and Freedom of Information, Germany

Co-Sponsors:

Privacy Commission, Belgium

Privacy Commissioner of Canada

Information and Privacy Commissioner of Ontario/Canada

Information Commissioner, United Kingdom

Institute for Access to Information, United Mexican States

Today the Internet has become the main technology for transporting every kind of communication, whether voice, video or data, and the basis for almost all business transactions and social interactions. Given the imminent exhaustion of the addresses provided by IPv4 Internet Protocol version 4), the protocol currently used for connecting to the Internet, given the continuing enormous demands for Internet addresses in the world and given the need for the Internet to support an increasing array of new devices, including sensors and smart meters(the 'Internet of Things'), a new Internet Protocol, (IPv6 – IP version 6) has been standardised, developed and tested during the last 10 years and now needs to be implemented.

Although IPv6 presents a number of practical advantages over IPv4 its characteristics can also lead to specific privacy and security risks, which depend on the configuration of the new protocol and especially on the IPv6 address allocation and assignment strategy chosen. These risks should be addressed and controlled as the new Internet protocol version is deployed.

The International Conference makes the following recommendations:

- The use of temporary and volatile IPv6 addresses ("*dynamic addresses*") should remain possible for any user by keeping the dynamic assignment of IPv6 addresses by ISPs. Internet Access Providers and operators of gateways should offer the use of dynamic IP addresses as a default. Users should also be able to change their IP address during a session though a simple procedure. Legislators or regulators, as appropriate, should consider adding respective obligations to their national regulatory frameworks where this is not already the case.
- The use of temporary and volatile IPv6 addresses should remain possible with the IPv6 auto configuration features by using all the existing possibilities of pseudo randomisation of the interface identifier ("*privacy extensions*"). Equipment manufacturers – and specifically those of mobile devices - should swiftly incorporate such facilities in their products. The use of dynamic addresses for terminal equipment should be activated as a default feature
- By default providers, protocols, products and services should offer the choice to use temporary and volatile addresses.
- As appropriate, networks and applications should fully utilise all the security features of IPv6 (IPSec) to ensure security, integrity and confidentiality.
- Whenever location information is necessary for the use of services on mobile devices and other objects connected via IPv6, such information should be protected, such as by encryption, against unlawful interception and misuse.
- All actors responsible for the elaboration and the implementation of any further evolution of the IP protocol must ensure that any such standards and specifications fully consider privacy and data protection rights and values from the beginning.

The International Conference welcomes that the International Working Group on Data Protection in Telecommunications (IWGDPT) is at present discussing a comprehensive report on these issues. The report should especially examine the effects of a privacy friendly implementation of IPv6 on the area of law enforcement. The IWGDPT is asked to finalize its report in the light of the above mentioned recommendations.