EU public consultation by the RIPE NCC

I. Introduction

The European Commission launched a public consultation on the legal framework for the fundamental right to protection of personal data by posing three questions to the public:

- *"Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalization"*
- *"In your views, the current legal framework meets these challenges?"*
- *"What future action would be needed to address the identified challenges?"*

The RIPE NCC welcomes this opportunity for public consultation and supports the consultation by presenting its view. Before replying to these questions, we would like to provide some information about the RIPE NCC.

The Réseaux IP Européens Network Coordination Centre (RIPE NCC) is an independent, not-for-profit membership organisation. Most of the RIPE NCC's members are Internet Service Providers (ISPs) and telecommunication organisations. Other members are large corporations, academic institutions and government bodies[1].

The RIPE NCC supports the operation and development of the Internet through technical coordination and operates one of the world's five Regional Internet Registries (RIRs). It is an open, transparent and neutral organisation. The RIPE NCC operates as a community-driven, bottom-up and self-governing organisation. The policies that govern the way the RIPE NCC operates are proposed, discussed and accepted by the RIPE community[2]. The RIPE NCC's most prominent tasks include:

- Distribution and registration of IP addresses and Autonomous System (AS) Numbers
- Operating the RIPE Database
- Coordinating the RIPE community

The RIPE NCC plays a crucial role in the operation of the global Internet and can, therefore, provide the European Commission with useful insights. Additionally, a specific task force, the RIPE Data Protection Task Force, was established in 2006 and concluded its work recently on data protection. In particular, this task force examined the European Data Protection regulations and implemented ways to

[1] For more information about the RIPE NCC, see www.ripe.net

[2] RIPE (Réseaux IP Européens) is a collaborative forum open to all parties interested in wide area IP networks. The objective of RIPE is to ensure the administrative and technical coordination necessary to enable the operation of the Internet within the RIPE NCC service region. For more information about the RIPE community, see http://www.ripe.net/ripe/

ensure that registry data in the RIPE Database complies with relevant Data Protection regulations[3].

The Data Protection Directive, as mentioned by the European Commission, does not separately address Data Protection issues raised by technologies such as the Internet[4]. The RIPE NCC will present some aspects of the Internet environment that might impact upon personal data protection, and it will address the questions posed by the EU Commission separately for each aspect.

II. IP addresses as personal data

a) IP addresses

An Internet Protocol (IP) address is a numeric identifier that includes information about how to reach a network location via the Internet routing system. On its own, an IP address does not provide information about the identity of who is using the IP address, the exact location of the user or the purpose for which the IP address is being used. The RIPE NCC acknowledges that long discussions have taken place on whether an IP address can be considered as personal data or not. Both opinions have been strongly supported.

b) Does the current legal framework address this issue?

The current legal framework does not examine the status of IP addresses in particular. But Article 2(a)1 of European Directive 95/46/EC provides:
"… personal data shall mean 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 …"

Recital 26 further explains this concept:
"… whereas, 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;
whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."

The position of the RIPE NCC is the following: whether it is static or dynamic, an IP address as such does not directly provide any information about the identity of an individual user. The identification of the user depends only on other information, apart from the IP address, that can be obtained and associated with the IP address by the controller or by any other person. Without the right combination of information, it is impossible for an IP address to lead even

[3] For more information about the RIPE Data Protection Task Force, see http://www.ripe.net/ripe/tf/dp/index.html
[4] Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (COM(2007) 87 final), p.7

indirectly to the identification of an individual and, therefore, an IP address should be considered anonymous information.

The RIPE NCC considers that only a limited number of persons are in the position to possess and to combine with reasonable means the relevant information that links an IP address with an individual user. For example, the ISP who has connected a user with a particular IP address based on a contractual relationship can identify an individual by combining all personal information that the user provided for the performance of the contract. But if an ISP does not have a contractual relationship with the individual user, for example when the individual makes use of a free wireless connection or if the contract has been signed not by a user but by a legal entity, then not even an ISP has enough information to make this combination.

An IP address can be considered personal data only indirectly and only under specific conditions. To conclude that IP addresses are always personal data just because some persons under certain circumstances can identify the individual user would be inappropriate and disproportional, because by possessing the right combination of information, anything could be considered as personal data.

c) Proposal

The RIPE NCC believes that the legal framework as it is now is sufficient in this respect and would advise against a radical change to the legal framework that would lead to a conclusion whereby "all IP addresses are personal data". Such a consideration would not be in line with the purposes of the Data Protection regulations.

III. Loading personal data onto the Internet

a) Transferring vs loading of personal data in the Internet environment

The RIPE NCC recognises a distinction between transferring data to a defined recipient on the one hand, and loading data on an Internet webpage on the other hand. Once an object is loaded onto an Internet webpage, it can be visible and accessible by anyone in the world that has access to this webpage. The data controller in this case is not in a position to control who might have access to the personal data and further process it.

b) Does the current legal framework meet this challenge?

The European Directive 95/46/EC, in Chapter IV, has provisions regarding the transfer of personal data to third countries. Once personal data is loaded on a webpage, it is accessible in third countries. The Directive has not explicitly foreseen this aspect. However, the European Court of Justice (ECJ) has come up with an interpretation:
"*there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto*

an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country". [5]

The RIPE NCC welcomes this interpretation. Indeed, if the loading of information on the Internet means transfer of data, then the Member States should be obliged to prevent any personal data being placed on the Internet, which would lead to a disproportional restriction.

As long as individuals give their consensus for their personal data to be loaded onto an Internet webpage, they should be aware of the fact that their data might be accessible from anywhere.

c) Proposal

The RIPE NCC finds the ECJ interpretation of the current legal framework sufficient and would advise against any change to that interpretation.

IV. Internet resources administration

a) Contact details of people responsible for maintaining Internet connectivity and communication

IP addresses and Autonomous System Numbers (ASNs) are referred to as Internet Number Resources (INRs). For the proper functioning of the Internet, INRs must be unique. To ensure uniqueness, INRs need to be allocated and registered in an organised manner. This role was initially taken on by the Internet Assigned Numbers Authority (IANA) at the beginning of the 1990s.

As the Internet grew, it became clear that the IANA could not meet the demand for INR allocation and the range of different regional needs. The five Regional Internet Registries (RIRs) emerged to manage the allocation, assignment and registration of INRs within specified global regions. Each RIR has the active support of its regional Internet community and has the authority to administer and register INRs.

The registration of INRs does not refer to the registration of the actual user of a specific device connected to the Internet. It refers to the registration of the organisation (for example, the ISP) that is responsible for the maintenance of networks that correspond to blocks of IP addresses and ASNs. To facilitate communication among persons responsible for networks in case of a technical disorder, every registered organisation is obliged to provide and to keep updated the professional contact details of persons that, because of their profession, are responsible for the administration and the technical maintenance of each network. These contact details are very important for the smooth and

[5] European Court of Justice: C-101/01 (judgment of 6 November 2003) / Reference for a preliminary ruling from the Göta hovrätt: Bodil Lindqvist, par.71

uninterrupted operation of Internet connectivity. It should be stressed once again that these persons have nothing to do with the actual users of a device.

b) Does the current legal framework meet this challenge?

The European Directive 95/46/EC in Chapter IV provides restrictions regarding the transfer of personal data in third countries. In particular, according to Article 25, Paragraph 1: "… *the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if … the third country in question ensures an adequate level of protection.*"

However, the global dimension of the networks that interact in order for the Internet to function is not compatible with the geographical limitations of this provision. For the Internet to be globally available, the personal details of people responsible for the uninterrupted functioning of Internet networks need to be available outside the European Union.

c) Proposal

The RIPE NCC considers that personal data related to the operators of the Internet should be easily available to each other, both inside and outside the EU, in order for those individuals to be able to contact one another to coordinate the proper functioning of the Internet around the world.

V. Conclusion

The RIPE NCC, as an organisation with a unique and crucial position in the Internet community, as well as experience with data protection issues, is taking part in the public consultation organised by the European Commission and, for the aforementioned reasons, it states the following:

- There should be no radical change that causes the legal framework to provide that all IP addresses under any circumstances are personal data because this would be inappropriate and disproportional.
- The RIPE NCC supports the ECJ's current interpretation that loading personal data onto the Internet should not be considered as transferring of personal data.
- The Internet is global and, therefore, the contact details of any employees designated to be the contact point for the administrative and technical support of a network or group of networks should be globally available for the purposes of the uninterrupted functioning of the Internet.