BSA
BUSINESS SOFTWARE ALLIANCE

Brussels, October 8th 2008

Online Security, Traffic Data and IP Addresses

Review of the Regulatory Framework for Electronic Communications

Francisco Mingorance
Senior Director
Government Affairs
franciscom@bsa.org

Sq. de Meeûs 38/40
B-1000 Brussels
T +32 2 401 6808
F +32 2 403 1328

At the occasion of the Review of the Regulatory Framework for Electronic Communications and Services, the Business Software Alliance encourage the EU Council to **(1) define the rules applicable to the processing of traffic data for the purpose of online security and (2) to clarify when IP addresses are personal data.**

The Review of the Regulatory Framework for Electronic Communications and Services provides a unique opportunity to enhance online security in Europe. A secure online environment is essential to protect both European consumers and businesses. When citizens or businesses use services online, their personal data must be safe and security measures must be readily available to prevent the disruption of network operations, the slowing down or denial of services. If users do not have confidence in the security and reliability of online services, they will not use the Internet nor harness the full potential of the European Information Society. This, in turn, is likely to harm economic growth and continued innovation in the online sector.

As described in more detail below, we suggest that:

- **There is a need to clarify the legal framework for the processing traffic data, including IP addresses, for security purposes.** The e-Privacy Directive does not include a clear legal basis for processing of traffic data for security.

- **The status of IP addresses under EU data protection law should also be clarified.** The Article 29 Working Party has stated that in some cases, IP addresses are personal data and in others they are not. Member State rules are likewise not uniform.

- **The legal uncertainty surrounding the processing of traffic data and the status of IP addresses threatens online security and puts users at risk**. Many security systems used by banks, retailers, governments and other service providers rely on their ability to process traffic data, including IP addresses. A clear legal basis is therefore needed for such activities.

- **Amendments approved by Parliament addressing these issues remain insufficient.** The provision on processing of traffic data (IMCO Amendment 181) may not provide the legal certainty needed to ensure online security. On the crucial question of the status of IP addresses under EU law, the Parliament is merely calling for a study (IMCO 185 and 186).

Why is the legal framework for the processing of traffic data for security purposes unclear?

- **The e-Privacy Directive does not include a clear legal basis for processing of traffic data for security purposes.** This Directive requires operators of public electronic communications services and networks to erase or make anonymous traffic data when it is no longer needed for the purpose of the transmission of a communication (Art. 6(1)). It also provides a limited number of exceptions to this obligation in Article 6 and Art. 15(1). While some of these exceptions might arguably apply to processing of traffic data for purposes of network security, this is not entirely clear. For example, while there is an exception for the "unauthorised use of the electronic communication system," the scope of this exception is uncertain.

- **It is also questionable whether the current exemptions permit processing for security purposes by information society services (web pages engaged in e-commerce) or by security services operating on behalf of others, including for the protection of home users.** Currently, such exemptions only extend to the operators of public electronic communications services and the entities acting on their behalf. With the increasing number of online services created over the last few years, operators of public electronic communications services cannot be expected to provide network security for each and every new service, nor can the task of securing such new services rest solely on their shoulders.

Why is the status of IP addresses under EU data protection law unclear?

- **The Article 29 Working Party has stated that in some cases, IP addresses are personal data and in others they are not.** Broadly, the Article 29 Working Party in its published opinions takes the view that if an individual can be identified from the data, albeit with great legal or technical difficulty, then the data is "personal data" and subject to all the relevant limitations. From a practical point of view, this makes little sense, as there is not a realistic possibility in many cases that the party holding the IP address could obtain the information needed to link the IP address with an individual.

- **Furthermore, many Member States have interpreted the e-Privacy Directive as prohibiting ISPs from divulging user information connected to IP addresses except in very limited cases – meaning that most third parties do not and will not have access to information that permits the IP address to be associated to an individual.** If a third party cannot receive assistance from an ISP and has no other way of associating an IP address with a particular user, the IP address is not personal data as far as the third party is concerned. The UK has adopted a pragmatic approach to this issue, deeming data personal if the individual to whom they relate is identifiable "from those data and other information in the possession or likely to come into the possession of the data controller." (UK Data Protection Act 1998, section 1(1)). Other countries like Germany have adopted a similar view.

What are the consequences of this legal uncertainty for online security?

- **Security technologies and systems rely on the processing of traffic data to keep data and users safe.** Organisations must continuously monitor their networks for, and defend against, security threats, including denial of service attacks, hacks, viruses and other forms of system infiltration. To enable this, security systems monitor and collect traffic data from various points in the network, such as sniffers, routers, firewalls, intrusion detection systems and servers. By analysing this data, firms can identify patterns of activity, distinguish normal traffic from suspicious activity, and anticipate or detect network attacks. Analysis of this data allows online service providers to protect the victims of an attack and to stop or prevent such attack from occurring again.

- **Traffic data processed for security purposes is largely "anonymous."** For example, financial services institutions that provide e-banking constantly analyze and process traffic data that affect their online services, the majority of which is generated by individuals who are not clients of the bank and who cannot be identified directly by the bank based on the traffic data. Processing this anonymous traffic data allows the institution to provide online security services that prevent ill-intended individuals from testing and breaking into the bank's system, and ultimately from stealing money from its customers.

- **The processing of traffic data is required to ensure a safe Internet.** Banks, hospitals, retailers, IT companies, businesses engaged in e-commerce activities and governments all process anonymous traffic data to prevent malicious attacks and information security breaches. If anonymous traffic data cannot be processed for deploying and providing security solutions for online services, the Internet becomes a space where unlawful individuals can steal personal data from legitimate users in virtual impunity.

Why are the amendments passed by Parliament insufficient to address these issues?

Parliament approved an amendment (IMCO 181) aimed at permitting the processing of traffic data for security purposes. This amendment incorporated several of changes proposed by the European Data Protection Supervisor,[1] as well as additional language. These changes threaten to undermine the effectiveness of the provision and we encourage the Council to consider alternative solutions. Our principal concerns include the following:

- **The Amendment (IMCO 181) strongly implies that traffic data are personal data in all instances.** In particular, by inserting the term "data controller" into the provision, Parliament is in effect legislating that traffic data, and the IP addresses within them, are always personal data. As the EDPS recognises in its Comments, however, "whether a piece of information ... constitutes personal data or not must be assessed on a case-by-case

[1] *EDPS Comments on Selected Issues that Arise from the IMCO Report on the Review of Directive 2002/22/EC & Directive 2002/58/EC*.

basis" (para. 8). Ultimately, the language adopted by Parliament could lead to data protection authorities and courts applying certain rules applicable to personal data that would make the task of providing effective security more difficult. For example, hackers could have the right to access traffic data collected about them and to "rectify" what they view as errors in the data -- a clearly nonsensical outcome.

- **The text would give hackers and cyber criminals the right to challenge processing activities.** In language that goes beyond what was recommended by the EDPS, Parliament has provided that the authority to process traffic data for security purposes is overridden by "the interests for the fundamental rights and freedoms of the data subject." This language would also provide an explicit basis for hackers and cyber criminals to launch frivolous litigation intended to harass businesses and security providers that are attempting to ensure a safe online environment.

- **By specifying that processing must be done "for the legitimate interest of the data controller," the revised amendment is overly narrow and may prevent processing by all of the persons who need to do so to ensure a safe online environment.** Any natural or legal person with a legitimate interest, including third party service providers and home users whose security software interacts with a service provider's servers, should be covered by the provision, regardless of whether they are deemed a data controller or deemed to be acting on behalf of one.

With respect to the legal status of IP addresses, Parliament rejected a recital that would have helped clarify the circumstances under which IP addresses should be deemed personal data for purposes of the e-Privacy Directive (IMCO 30). Instead, Parliament is calling for a study to be undertaken on the application of the e-Privacy Directive to IP addresses (IMCO 185 and 186).

The uncertainty concerning the circumstances under which traffic data may be legally processed and the status of IP addresses threatens the ability of many providers to operate essential security systems and puts the safety of users of online services at risk.

To eliminate this uncertainty, two solutions are necessary: (1) A clear exception for the processing of traffic data to preserve network and information security; and (2) A clarification of when IP addresses are personal data.

(1) A clear exception for the processing of traffic data to preserve network and information security.

Our proposed text in Annex A would address the shortcomings Identified above in the Parliament's amendment. It would ensure that any natural or legal person may process IP addresses for security purposes. It would also ensure that the provision covers processing by information society services (web pages engaged in e-commerce).

While the proposed text we support does not suggest that IP addresses are always personal data, it does include important safeguards to protect users. Processing must be for the purpose of "technical measures to ensure the security" of online services and related equipment, and such processing "must be restricted to that which is strictly necessary for the purposes of such

security activity." It is also clear that the provision does not exempt the processing of traffic data for security purposes from compliance with all of the provisions of the ePrivacy and Data Protection Directives – safeguards on the use of this data thus remain.

(2) A clarification of when IP addresses are personal data

If IP addresses are deemed to be personal data in many circumstances, it could lead to considerable disruption of the Internet. For example, if a user connects with a web page that provides a weather forecast, the full range of data protection rules could apply to the user's IP address. The web site operator would be subject to notice and consent requirements, and would be legally obligated to, upon demand, provide the user with access to data held on the user and to correct that data. This would seem unduly burdensome given the nature of the contact the user had with the web site and could arguably paralyze the technical functioning of Internet-based services.

For this reason and in conjunction with the proposed European Commission study and recommendations on standard uses of IP addresses and the application of the e-Privacy Directive as regards their collection and further processing (IMCO 186), we urge the Council to add a recital that would help clarify when IP addresses are deemed personal data for purposes of the e-Privacy Directive. Significantly, this clarification should not preclude the case-by-case analysis of whether an IP address is personal data, which the EDPS has indicated is important given the evolving nature of online services, nor should it lower the existing level of protection available under the e-Privacy Directive. Instead, it would clarify how these case-by-case determinations are to be made (See Annex B)

Annex A

Revise the Council's Proposed Text

Proposal for a directive - amending act
Article 2 - point 4 b (new)
Directive 2002/58/EC
Article 6 - paragraph 6a (new)

Commission	*Original Parliament Amendment*	*Proposed Text*
N/A	6a. Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive, traffic data may be processed for the legitimate interest of the data controller for the purpose of implementing technical measures to ensure the network and information security, as defined by Article 4 (c) of Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency[1], of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment, except where such interests are overridden by the interests for the fundamental rights and freedoms of the data subject. Such processing must be restricted to that which is strictly necessary for the purposes of such security activity.	6a. Traffic data may be processed **by any natural or legal person with a legitimate interest** for the purpose of implementing technical measures to ensure the security of a publicly available electronic communication service ~~or~~**,** a public electronic communications network, **an information society service,** or related terminal and electronic communication equipment. Such processing must be restricted to that **which** is strictly necessary for the purposes of such security activity.

Justification: Third party providers of security services, and home users whose security software interacts with a service provider's servers, should be able to process traffic data for security purposes. Furthermore, information society services face many of the same security threats as electronic communication services and networks, and should therefore also be covered by this provision.

Annex B

Revise IMCO Amendment 185

Proposal for a directive - amending act
Recital 27 a (new)

Commission	*Original Parliament Amendment*	*Proposed Text*
N/A	(27a) IP addresses are essential to the working of the internet. They identify network participating devices, such as computers or mobile smart devices by a number. Considering the different scenarios in which IP addresses are used, and the related technologies which are rapidly evolving, questions have arisen about their use as personal data in certain circumstances. The Commission should therefore conduct a study regarding IP addresses and their use and present such proposals as may be appropriate.	(27a) IP addresses are essential to the working of the internet. They identify network participating devices, such as computers or mobile smart devices by a number. Considering the different scenarios in which IP addresses are used, and the related technologies which are rapidly evolving, questions have arisen about their use as personal data in certain circumstances. ~~The Commission should therefore conduct a study regarding IP addresses and their use and present such proposals as may be appropriate.~~ ***For the purpose of Directive 2002/58/EC, an Internet Protocol addresses should be considered as personal data only if it, alone or in conjunction with other data, relates to an individual directly identifiable by the entity processing the IP address.***

Justification: If IP addresses are always considered to be personal data it may disrupt the functioning of online services. If an IP address cannot be directly linked to an individual, there is no risk to privacy. This amendment helps clarity the circumstances under which IP addresses should be considered personal data.