28 October 2008

Position on the processing of traffic data for "security purposes"

Summary

1. At the occasion of the Review of the Regulatory Framework for Electronic Communications and Services, the Working Group on Data Retention asks the EU Council to (1) preserve the current rules applicable to the processing of traffic data and (2) preserve the current definition of personal data which encompasses IP addresses.
2. Amendment 181 to directive 2002/58/EC would expose a potentially unlimited amount of sensitive, confidential communications data to risks of disclosure or abuse. Amendment 181 needs urgently to be rejected by the Council.

I. No retention of traffic data for "security purposes" (amendment 181)

1. Vulnerability of telecommunications data

In recent years, Europe has suffered from several accidental and intentional disclosures and abuses of information on our communications, movements and Internet use, for example in Germany,[1] Italy,[2] Greece,[3] Latvia,[4] Bulgaria,[5] Slovakia[6] and Hungary.[7] These incidents have reminded us of the fact that only erased data is safe data. It has proven right the strict European regulations regarding the processing of traffic data. Limiting the collection of traffic data helps minimize the damage resulting from data leaks and has proven to effectively maintain our safety from abuse of communications data.

1 http://www.dw-world.de/dw/article/0,2144,3690132,00.html.
2 http://en.wikipedia.org/wiki/SISMI-Telecom_scandal.
3 http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005.
4 http://www.baltictimes.com/news/articles/18576/.
5 http://www.novinite.com/view_news.php?id=17103.
6 http://www.freemedia.at/cms/ipi/freedom_detail.html?country=/KW0001/KW0003/KW0080/&year=2003.
7 http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559531.

2. Data protection and economic growth

In view of the increasing number of disclosures and abuse of communications data citizens need to be reassured that the amount of data exposed to such risks is being kept as small as possible. Otherwise, citizens will not use the Internet nor harness the full potential of the European Information Society. This, in turn, would harm economic growth and continued innovation in the on-line sector.

3. Scope of regulations on traffic data

Article 6 of directive 2002/58/EC provides that "traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication [...]". This principle of erasure lies at the heart of the ePrivacy directive and makes sure that as little data as possible is being exposed to the numerous risks mentioned above.

It is important to realise the scope of Article 6. It only applies to providers of a "public communications network or publicly available electronic communications service". Article 2 (c) of directive 2002/21/EC defines "electronic communications services" as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks [...] exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services".

4. Regulations not applicable to Internet content providers

The regulations on traffic data do thus not apply to Internet content providers such as e-commerce companies, banks or retailers. Claims that IP addresses or other traffic data are needed by content providers for "security purposes" are therefore entirely irrelevant with regard to Article 6 of directive 2002/58/EC. As these claims have led to the introduction of amendment 181, this amendment is lacking a relevant basis.

Besides, we know of major German content providers that safely and reliably offer Internet content without collecting IP addresses or other traffic data. In fact, in a landmark ruling against the German ministry of justice, a Berlin court held in 2007 that "security needs" did not justify a blanket collection of the IP addresses and other traffic data pertaining to visitors of Internet

content.[8] The ministry had to change its policy and has since safely and reliably run its website without gathering any personal traffic data.

5. Regulations not applicable to attacks

The regulations on traffic data are limited to "data relating to subscribers and users". "User" means any natural person using a publicly available electronic communications service, for private or business purposes (Article 2). A person or a computer system attacking another computer cannot be said to be using the service provided and therefore falls outside the scope of Article 6.

6. Regulations not applicable to anonymous data

Furthermore, Article 6 allows anonymous traffic data to be used for "security purposes". Anonymous data allows for a sufficient monitoring of network traffic.

7. No need for fixed line and mobile telephony providers to collect traffic data for "security purposes"

Certain parts of the industry claim that non-anonymous traffic data was needed to defend against denial of service attacks, hacks or viruses on the Internet. These threats do obviously not concern fixed line and mobile telephony services. Yet, amendment 181 is not limited to Internet services.

8. No need for Internet communications providers to collect traffic data for "security purposes"

Providers of Internet communications services such as Internet access, Internet telephony or Internet e-mail do not need to collect non-anonymous information on their users for "security purposes". Denial of service attacks, hacks, viruses or other infiltrations cannot be prevented by collecting data. Instead, the providers' hardware and software needs to be configured safely. Safety mechanisms such as firewalls or software updates do not require personal data to work.

The absence of a need for collecting traffic data is proven by the successful application of directive 2002/58/EC. The Commission has rightly not proposed any changes to its regulations regarding traffic data.

9. Sufficient exceptions provided for in Article 15

According to Article 15 of directive 2002/58/EC, member states may provide for exceptions where necessary for the prevention, detection and investigation of unauthorised uses of an electronic

8 AG Berlin, judgement of 27 March 2007, 5 C 314/06.

communications system. Denial of service attacks, hacks, viruses and other infiltrations clearly constitute an unauthorised use of the attacked systems.

Member states therefore have introduced exceptions in a carefully balanced way. For example, the German Telecommunications Act allows for the processing of traffic data where an unauthorised use of a service is taking place (section 100 TKG). In a landmark case involving major Internet access provider T-Online, the courts have held that traffic data could only be collected on a case by case basis whereas a blanket collection of all customers' communications data for "security purposes" was illegal.[9]

Amendment 181, however, is not limited to actual incidents.

10. Amendment 181

While the Commission had intended to maintain the successful regulation of traffic data, the European Parliament has carved in to lobbying by parts of the industry and passed amendment 181.[10] This proposal would allow telecommunications providers to collect sensitive information on our communications, movements and Internet use "for the purpose of implementing technical measures to ensure the network and information security". The Parliament does not give any reasons for the proposal. The EDPS had advised against the adoption of amendment 181.[11]

11. Disastrous effects of Amendment 181

Amendment 181 is worded so broadly and imprecisely that providers would be able to potentially collect all traffic data for an unlimited period of time with the mere claim of the data being necessary for "security purposes". The amendment would render the principle of Article 6 (1), according to which traffic data must not be retained any longer than needed for the processing of a communication, meaningless. It would give a blank cheque to providers.

We have serious doubts whether amendment 181 meets the requirement of precision of the law, and whether it is compatible with the right to privacy (Article 8 ECHR) and the principle of proportionality.

9 LG Darmstadt, judgement of 7 December 2005, 25 S 118/2005.

10 European Parliament legislative resolution of 24 September 2008, P6_TA-PROV(2008)0452.

11 Comments of 2 September 2008, http://www.edps.europa.eu/.

12.Conclusion

As amendment 181 would expose highly sensitive data on our communications, movements and Internet use to risks of disclosure and abuse, it should urgently be rejected. The current protections have proven to constitute the best guarantee for our safety in information society.

II. IP addresses are personal data

1. Industry lobbying and its purpose

Certain parts of the industry are lobbying for a provision that would largely exclude IP addresses from the scope of data protection law. This is to enable Internet content providers to collect, pass on and disclose data on our Internet use ("click stream") without any limits. Whatever we read, search for or write on the Internet would be on the record for an unlimited period of time and could be traced to us by government authorities, ISPs and others.

2. Misplaced lobbying

First of all, this lobbying is systematically misplaced. The telecommunications package is not the right place to define what constitutes personal data. As mentioned above, the Internet content providers that would like to collect traffic data are not providers of telecommunications services and are thus not covered by the telecoms package.

3. The status of IP addresses is already clearly defined

The right place to define what constitutes personal information is the directive 95/46/EC on data protection. In recital 26, it contains a clear definition of personal data: "*Whereas the principles of protection must apply to any information concerning an identified or identifiable person; 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 article 29 group has rightly held that Internet access subscribers can easily be identified by their IP address, especially taking into account the data collected by Internet service providers under directive 2006/24/EC on data retention. In the landmark

ruling involving the German ministry of justice, the competent Court confirmed that IP addresses collected by an Internet content provider are personal data as "*by combining the personal data with the help of third parties it is possible in most cases without substantial difficulty to identify Internet users by the IP address. Negating the personal character of the data [...] would mean that this data could be passed on to third parties such as the access provider without restrictions who in turn could identify the user by their IP address, which would violate fundamental principles of data protection law. Besides the defendant's argument that a person is identifiable only when they can be identified using legal means cannot be accepted. The plaintiff rightly points out that it is the precise purpose of data protection law to protect from an abuse of data, which is why the Court does not consider such a restriction on the definition of identifiability justified.*"[12]

There is no reason why the common definition of personal data in directive 95/46/EC should be altered to benefit certain Internet content providers.

4. Not protecting IP addresses is dangerous

If IP addresses were not considered personal data, Internet content providers could collect, pass on and disclose data on our Internet use ("click stream") without any limits. Whatever we read, search for or write on the Internet would be on the record for an unlimited period of time and could be traced to us by government authorities, ISPs and others.

In "real life", nobody takes notes of what we read, what we write and what we buy. If using the Internet involved a total registration of similar activities, this would substantially weaken consumer trust and confidence in the Internet and, in turn, harm economic growth in the on-line sector.

5. Conclusion

Industry lobbying for excluding IP addresses from the scope of data protection law should be rejected.

12 AG Berlin, judgement of 27 March 2007, 5 C 314/06. In an obiter dictum, AG Munich, judgement of 30 September 2008, 133 C 5677/08 expressed a different view, but its ruling has not come into force.

III. One word on the Business Software Alliance (BSA)

1. No legitimate interest in the ePrivacy directive

Most of the current lobbying to erode proven European privacy standards is done by the BSA, a group representing the interests of the commercial software industry. We cannot identify a single BSA member that actually provides telecommunications services and thus falls within the scope of directive 2002/58/EC. The BSA is lobbying in a field it has no legitimate stake in. Communications providers, on the other hand, are not known to have voiced objections to current privacy regulations.

2. Dangers of approximating laws to US practises

Nearly all of BSA's members are based in the United States and are used to a complete lack of privacy safeguards applying to their operations. The software and operations of most BSA members are designed to collect a maximum of personal data about their customers in order to make the greatest profit from it. The US policy has resulted, for example, in sensitive communications data being freely available for purchase in the US. It has also resulted in communications providers never deleting any data on their customers. The confidential data in these massive databases constitutes a ticking time bomb and may at any time result in accidental disclosures or abuse of data pertaining to our private lives and business contacts.

The European approach of preventing data crime by strictly limiting the amount of personal data available has proven effective and should be strengthened, not watered down.

28 October 2008

About the Working Group on Data Retention

The Working Group on Data Retention is a German association of civil rights and privacy activists as well as regular Internet users that is campaigning against the complete logging of all telecommunications. On 11 October 2008, we organised an international “Freedom not Fear” day. Tens of thousands of Europeans participated in protests against excessive surveillance.

Homepage: http://www.vorratsdatenspeicherung.de/?lang=en

E-Mail: kontakt@vorratsdatenspeicherung.de