21 March 2009

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

Summary

1. Amendments to the ePrivacy directive 2002/58/EC currently proposed by the Council and by IMCO rapporteur Malcolm Harbour (am. 85), would result in the creation of vast data pools and thus expose a potentially unlimited amount of sensitive, confidential communications data to risks of disclosure or abuse. These amendments need urgently to be rejected.
2. The Working Group on Data Retention asks the European Parliament to preserve the current guarantees regarding the processing of information on our use of telephones, mobile phones, e-mail and the Internet (traffic data).
3. Of the amendments currently tabled in IMCO, amendment 85 should be rejected and amendment 150 should be adopted, with a view of striking down the proposed modifications of article 6 altogether as soon as possible.

Comparison Chart

	Council common position (art. 2 point 6)	Council compromise proposal	Harbour IMCO draft report (am. 85)	Svensson IMCO (am. 150)	Working Group compromise proposal (p. 13 below)	Current wording of directive (art. 15)
	16 Feb 2009	27 Feb 2009	4 Mar 2009	18 Mar 2009	21 Mar 2009	12 Jul 2002
1. Specifies in which situations providers may collect and store traffic data; does not legalize permanent blanket data retention	**NO**	**NO**	**NO**	**YES**	**YES**	**MS decide**
2. Purpose specified to be the protection of the provider's own systems	**NO**	**NO**	O	**NO**	**YES**	**MS decide**
3. Maximum retention period specified	**NO**	**NO**	**NO**	**YES**	**YES**	**MS decide**
4. User interest may outweigh provider interest	**NO**	**YES**	**YES**	**NO**	**YES**	**YES**
5. Retained data may not be used for any other purposes (purpose limitation)	**NO**	**NO**	**NO**	**YES**	**YES**	**MS decide**
6. Specifies who is to be allowed to process traffic data	**NO**	**YES**	**NO**	**NO**	**YES**	**MS decide**
7. Limited to telecommunications providers, excludes information society services and others	**NO**	**NO**	**NO**	**NO**	**YES**	**YES**
8. Disclosure of communications data excluded, confidentiality of telecommunications guaranteed	**NO**	**NO**	**NO**	**YES**	**YES**	**MS decide**
9. Member states may protect privacy better	**NO**	**NO**	**NO**	**NO**	**YES**	**YES**
Recommendation	– – –	– –	– –	+	+ +	+ + +

No retention of traffic data for "security purposes" (proposed amendments to article 6 of directive 2002/58/EC)

1. Telecommunications data

When we talk to our family and friends, our business partners, our therapist or to other professionals, nobody takes note of our contact or whereabouts. When we read a newspaper or watch TV, nobody takes note of our habits and interests. Yet, when we use our telephone, mobile phone or the Internet for similar activities, the service provider has access to such information for technical reasons. Such "traffic data" allows most of our social contacts, our geographical movements and our Internet use to be meticulously retraced and revealed.

The collection of such information by private companies is not only comparable to a CCTV recording of our conversations, movements and media use. Traffic data is directly linked to our identity and can be automatically processed and evaluated. Whom we know, where we go and what we do on the Internet reflects our personalities, our preferences and our weaknesses in unprecedented detail. The European Parliament has therefore rightly provided us with special protection from the collection and dissemination of such information by adopting article 6 of directive 2002/58/EC.

2. 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.

3. 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.

4. The principle of erasure

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.

Article 6 is a specific and complete provision (*lex specialis*) which does not leave room for data processing under other directives such as directive 95/46/EC. Unlike Article 7(f) of directive 95/46/EC, the ePrivacy directive does not permit the processing of traffic data "for the legitimate interest of the data controller". This is because traffic data is much more sensitive than other data, revealing our personal and business contacts, our movements (cell IDs) and our Internet usage. In an information society, communications data is the key to our private lives. It can only be effectively protected by immediate erasure, as demonstrated by the numerous disclosures and abuses mentioned above.

5. Regulations not applicable to Internet content providers

It is important to understand 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".

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 the proposed amendment to article 6, this amendment is lacking a relevant basis. Article 7 (f) of directive 95/46/EC already permits Internet content providers to process personal data where "necessary for the purposes of the legitimate interests pursued by the controller".

6. 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.

7. 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.

8. 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, the proposed amendment to article 6 is not limited to Internet services.

9. 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 in the past.

10. 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 communications system.[8] Denial of service attacks, hacks, viruses and other infiltrations clearly constitute unauthorised uses 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]

The amendments proposed now, however, are not limited to actual incidents.

11. Council common position

In its common position dated 16 Feb 2009, the Council proposes amending article 6 as follows:[10]

> *"(6a) Traffic data may be **processed** to the extent strictly necessary 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."*

12. Council compromise proposal

On 27 Feb 2009, the Council Presidency proposed amending article 6 as follows:[11]

> *"1b. Traffic data may be **processed** by the data controller to the extent and for the time strictly necessary 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*

8 Article 29 working group, Opinion 1/2009 of 10 February 2009 (WP 159), 7.

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

10 Council document 15899/08 of 20 November 2008, adopted on 27 November 2008.

11 Council document DS 177/09 of 27 February 2009, http://www.laquadrature.net/files/DS177_9_2009_02_27_print.pdf.

Network and Information Security Agency,[12] *of a public electronic communication service or network, or related terminal and electronic communication equipment, except where such interests are overridden by the interests of the fundamental rights and freedoms of the data subject."*

13. The Parliament rapporteur's draft report for the second reading (IMCO amendment 85)

Although the Parliament's first reading proposal to amend article 6 (amendment 181) has attracted widespread criticism from civil society, professional organisations, data protection officials and the EDPS, IMCO rapporteur Malcolm Harbour intends to fully uphold the proposal. In his IMCO draft report of 4 March 2009, he proposes amending the Council common position as follows (amendment 85):

"1b. 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*** *in 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, 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 those of the fundamental rights and freedoms of the data subject. Such processing shall be restricted to that which is strictly necessary for the purposes of such security activity."*

14. MEP Svensson's proposal for the second reading (IMCO amendment 150)

According to an amendment tabled by Eva-Britt Svensson in IMCO, the Council common position is to modified as follows:

"7. Traffic data may be ***collected, stored and used in specific cases*** *to the extent strictly necessary to ensure*

12 Article 4(c) of Regulation (EC) 460/2004 reads: "'network and information security' means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems".

network and information security, as defined by Article 4(c) of Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. Traffic data stored pursuant to this paragraph ***must not be used for any other purpose and must be erased or made anonymous no later than seven days after its collection****."*

15. Disastrous effects of proposed amendments

Adopting the Council common position or the modification proposed by IMCO rapporteur Malcolm Harbour (amendment 85) would have disastrous consequences:

- The proposals do not specify in which situations providers would be allowed to collect and store traffic data. They are worded so broadly and imprecisely that providers would be able to potentially collect all of our communications data for an unlimited period of time with the mere claim of the data being necessary for "security purposes". The amendments 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. They would give a blank cheque to providers. They are not limited to the collection of data "in specific cases" of incidents but would permit a permanent blanket retention of most sensitive data on our private communications.

- The proposals do not specify precisely to what end communications data may be collected. The proposals are not limited to the protection of the providers' systems, but would legalize measures to purportedly promote "network and information security" in general. Providers would be allowed to filter and inspect our communications for "suspicious activity" or alleged "malicious actions" involving any computer on the Internet. Advocate General Juliane Kokott warned recently:[13] "*In order to be able effectively to verify whether electronic communication systems were being used for unauthorised purposes, it would be necessary to store the entire communication and process it intensively with regard to the content. The citizen 'under the eye of Big Brother' would thus be a reality.*"

- The proposals do not set a time limit for the retention of traffic data. If the proposals were passed in their current

13 Opinion delivered on 18 July 2007, Case C-275/06, § 97.

wording, communications providers would be able to collect information on our communications for a potentially unlimited period of time. This would correspond to US practices where many providers have never deleted any communications data since their establishment. In fact, communications data is freely being offered for purchase in the US. Europe would face similar "time bombs" of sensitive data if any of the proposed amendments is passed.

- The proposals do not limit the purpose of retained communications data. Providers would be able to collect information on our telecommunications under the guise of "information security" but use the data for entirely different purposes (e.g. serve requests by government authorities or the entertainment industry).
- The proposals do not specify who is to be allowed to collect traffic data. They are not clearly limited to communications providers and thus exceed the scope of the directive. It appears that any natural or legal person who can get hold of traffic data would be allowed to collect it for "security purposes", including content providers ("information society service") and employers.
- The proposals do not safeguard the confidentiality of telecommunications. The term "processing" covers the "disclosure by transmission, dissemination and otherwise making available" of traffic data.[14] The proposals would thus authorise the dissemination of our communications data to third parties. The Rapporteur's draft proposal even explicitly exempts the processing of traffic data from the confidentiality of communications guaranteed in Article 5 of directive 2002/58/EC.
- The proposals eliminate the ability of member states to decide autonomously and in line with their constitutional values, whether and to what extent the citizens' privacy should be sacrificed to business interests. Currently, many member states make no exceptions from the principle of erasure (article 6). Other member states have introduced exceptions that are far more precise and narrow than the European proposals tabled now.

We believe that none of the current proposals meets the requirement of precision of the law, and is compatible with the right to privacy (Article 8 ECHR) and the principle of

14 See Article 2 (b) of directive 95/46/EC.

proportionality. The European Court of Human Rights only recently found the "the blanket and indiscriminate nature of the powers of retention" of fingerprints in the UK "a disproportionate interference with the applicants' right to respect for private life".[15]

Traffic data reflect our contacts, movements and Internet use and are much more sensitive than fingerprints. They require the utmost protection by the legislator and must be deleted when no longer needed for the purpose of the transmission of a communication. In view of the highly sensitive nature of this data, there cannot be any exceptions; nor is there a need for any additional exceptions (see 4.-9. above).

16. Data protection supervisors, civil society position

In a letter of 29 October 2008, 11 civil liberties, journalists, lawyers and consumer protection organisations criticized that the amendment to art. 6 proposed in first reading by the European Parliament would give companies a "blank cheque" to collect more traffic data than is currently being collected even under the directive on data retention, without setting a time limit.[16] This would lead to the creation of unmanageable data dumps and ultimately "expose sensitive data on our communications and movements to risks of abuse." They asked the Council to reject the Parliament's proposal of article 6 (6a).

On 6/7 November 2008, the German Conference of Data Protection Commissioners asked the federal government to reject the Parliament's proposal in Council, stating:

> *"A blanket collection of traffic data is therefore unnecessary to ensure network and information security. [...] The Conference of the Federal and the Länder Data Protection Commissioners rejects a blanket power of that kind, unlimited in time and indefinite in content, and considers it unacceptable."*[17]

In his opinion of 9 January 2009, the EDPS "recommends to reject this Article".[18] He confirms that "Article 6.6(a) is unnecessary and subject to risk of abuse" and goes on to say:

15 Marper vs. UK, Judgement of 4 December 2008.

16 http://www.vorratsdatenspeicherung.de/content/view/271/79/.

17 http://www.bfdi.bund.de/cln_027/nn_533554/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBundLaender/76DSK__RLElektronischeKommunikation,templateId=raw,property=publicationFile.pdf/76DSK_RLElektronischeKommunikation.pdf.

18 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf, p. 13.

> *"Any existing or future article is unlikely to remove the obvious risks of an overly broad application of the exception for reasons other than purely security related or by entities that should not be able to benefit from the exception. [...] Taking into account on the one hand the risks that Article 6.6(a) poses to the fundamental right to data protection and privacy of individuals, and on the other hand the fact that, as explained in this Opinion, from a legal point of view, this Article is unnecessary, the EDPS has come to the conclusion that the best outcome would be for the proposed Article 6.6(a) to be deleted altogether."*

In a joint press release of 29 January 2009, several privacy NGOs urged the European Parliament to heed the advice given by the European Data Protection Supervisor and drop the proposed amendment.[19]

In an opinion of 10 February 2009, the article 29 data protection working party warned that the proposed amendments could lead to "large scale deployment of deep packet inspection".[20] The working party confirmed that there is already a legal basis for security measures in Article 15 (1) and that therefore, "the proposal for a new Article 6(6a) is unnecessary."

In an opinion of 6 March 2009, the German Federal Assembly (Bundesrat) rejected a similar proposal by the German government and decided that the processing of traffic data for "security purposes" should only be allowed on a case-by-case basis where necessary to eliminate a fault in the provider's network. Any data collected to that end should not be used for any other purpose and not be disclosed to third parties.[21] The competent committee had furthermore recommended to set a time limit of 24 hours on the retention of traffic data for "security purposes".[22]

19 http://www.vorratsdatenspeicherung.de/content/view/295/79/.

20 Article 29 working group, Opinion 1/2009 of 10 February 2009 (WP 159), 7.

21 Bundesrat, Recommendation of 6 March 2009 (BR-Drs. 62/09), http://www.bundesrat.de/cln_090/nn_8336/SharedDocs/Drucksachen/2009/0001-0100/62-09_28B_29,templateId=raw,property=publicationFile.pdf/62-09(B).pdf.

22 Bundesrat, Committees' recommendations of 24 February 2009 (BR-Drs. 62/1/09), http://www.bundesrat.de, 9.

17. Recommendations

As the proposed amendments to article 6 would result in the creation of vast data pools and thus expose a potentially unlimited amount of highly sensitive data on our communications, movements and Internet use to risks of disclosure and abuse, they should urgently be rejected. The current protections have proven to constitute the best guarantee for our safety in information society.

In the European Parliament's the second reading, the following amendment to the Council common position of 16 February 2009 should be tabled and adopted:

> *"Council common position*
> *Article 2 – point 6*
> *Directive 2002/58/EC*
> *Article 6*
>
> *Amendment:* ***Article 2 – point 6 shall be deleted****.*
>
> *Justification: In his opinion of 9 January 2009, the EDPS 'recommends to reject this Article'. He confirms that 'Article 6.6(a) is* ***unnecessary and subject to risk of abuse****' and goes on to say: 'Any existing or future article is unlikely to remove the obvious risks of an overly broad application of the exception for reasons other than purely security related or by entities that should not be able to benefit from the exception. [...] Taking into account on the one hand the* ***risks that Article 6.6(a) poses to the fundamental right to data protection and privacy*** *of individuals, and on the other hand the fact that, as explained in this Opinion, from a legal point of view, this Article is unnecessary, the EDPS has come to the conclusion that the best outcome would be for the proposed Article 6.6(a) to be deleted altogether.' The European Parliament shares this view."*

If it proves politically impossible to delete the proposed amendment altogether, it would need to be drastically reworded. It would need to be limited to the "collection, storage and use" of data "in specific cases" rather than permitting a permanent, indiscriminate retention and disclosure of data. It would need to be limited to the protection of the provider's telecommunications systems, set a time limit and provide for a purpose limitation. It would also need to leave it to the member states to decide autonomously and in line with their constitutional values, whether and to what extent their citizens' privacy should be sacrificed to

business interests. To this end, by way of compromise, the amendment to article 6 could be reworded as follows:

> *"**Member states may allow** providers of **public communications networks and publicly available electronic communications services** to **collect, store and use** traffic data **in specific cases** to the extent strictly necessary to ensure the **security of their telecommunications systems**, 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, except where such interests are overridden by those of the fundamental rights and freedoms of the data subject. **Traffic data stored pursuant to this paragraph must not be used for any other purpose and must be erased or made anonymous no later than seven days after its collection."***

Notwithstanding this compromise proposal, any amendment to the current rules on the processing of traffic data is unnecessary and dangerous for the reasons set out above. We urge all institutions involved to effectively prevent the exposure of highly sensitive data to risks of disclosure and abuse by deleting the proposed amendment to article 6 completely. The current protections have proven to constitute the best guarantee for our safety in information society.

Of the amendments currently on the table in IMCO, amendment 85 should be rejected and amendment 150 should be adopted, with a view of striking down the modifications to article 6 altogether at a later stage.

Appendix: Resolution adopted by the 76th German Conference of the Federal and the Länder Data Protection Commissioners on 6 and 7 November 2008 in Bonn

No blanket powers for the software industry

Currently, changes to the directive on privacy and electronic communications (2002/58/EC) are being debated at the European level. Among others, there is discussion whether a blanket processing of traffic data should be allowed for ensuring network and information security, e.g. for the prosecution of hacker attacks.

On the basis of the current directive, section 100 of the German telecommunications act (TKG) allows telecommunications providers to process data for the targeted elimination of malfunctions and prevention of abuse in specific cases. This provision has proven to be effective in practise. A blanket collection of traffic data is therefore unnecessary to ensure network and information security. Providers of telecommunications services are called upon to design their systems so safely that external attacks remain unsuccessful in the first place.

Although the Commission has not considered necessary any changes to the current directive, several member states, in accordance with suggestions by the software industry (Business Software Alliance), are proposing in Council to add a general power to the directive which would allow "every natural or legal person with a legitimate interest" to process traffic data "for the purpose of implementing technical measures to ensure the network and information security". This would not only allow the relevant service provider wishing to secure its own systems to collect traffic data beyond specific cases but would extend to practically everyone with an economical interest in data processing, especially manufacturers of security software.

The Conference of the Federal and the Länder Data Protection Commissioners rejects a blanket power of that kind, unlimited in time and indefinite in content, and considers it unacceptable. The mention of "information security" does not justify a nearly unlimited processing of traffic data even by third parties. The federal government is called upon to refuse its consent in Council to any watering down of the secrecy of telecommunications of that kind.

Source:
http://www.bfdi.bund.de/cln_027/nn_533554/DE/Oeffentlichkeitsarbeit/EntschliessungssammlungDSBundLaender/76DSK__RLElektronischeKommunikation,templateId=raw,property=publicationFile.pdf/76DSK_RLElektronischeKommunikation.pdf

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