15 September 2004

DG INFSO B.1: infso-b1@cec.eu.int
DG JAI D.2: jai-eu-forum-organised-crime@cec.eu.int

DG INFSO – DG JAI Consultation Document On Traffic Data Retention:

Response from EuroISPA

Introduction

Data retention is one of the most important issues ever faced by the Internet service provider (ISP) industry[1]. The implications of proposed measures to oblige ISPs to retain data for long periods could have a devastating effect on the whole industry. EuroISPA has consistently expressed the ISP industry's serious concerns to regulators, legislators, governments and other stakeholders. In this paper we once again outline the technical, legal and cost issues that EuroISPA does not feel are fully appreciated by proponents of data retention.

Data retention is a complex and sensitive issue that continues to divide opinion. Such divisions cannot be assigned solely to differences between interest groups: they continue to separate national governments, regulators and legislators. EuroISPA welcomes this official consultation period by the European Commission and encourages a sustained period of closer dialogue between the relevant stakeholders.

Discussions to date:

On behalf of its whole membership, EuroISPA has consistently taken a lead role in discussions on the subject of data retention. Our member associations also continue to be prominent voices in national debates. EuroISPA and its member associations have brought technical, regulatory, legal and business experts to discussions to explain technical feasibilities, existing legal and regulatory constraints and the serious business impact data retention has on an industry the European Union and its member states otherwise enthusiastically promote. EuroISPA has

[1] The term "Internet Service Provider" refers to all companies that are members of EuroISPA's member associations.

already expressed serious concerns about the recently tabled Draft Framework Decision from France, Ireland, Sweden and the United Kingdom, which we conclude is unworkable.

There can be no greater illustration of the whole communication service provider industry's concern than the consistent, joint messages expressed by associations such as EuroISPA, ECTA, ETNO and GSM Europe[2]. This united, pan-industry voice demonstrates communication service providers' alarm at the impracticable proposals produced to date.

EuroISPA and its member associations have always been constructive partners in discussions with law enforcement authorities (LEAs), governments and other stakeholders. This contribution to the European Commission's consultation stresses once again the critical importance of the issue to our industry. We underline, however, that it is impossible to cover every issue in extensive detail in this response and that it will be necessary to establish a framework to provide ongoing industry input to EU level discussions. Without such input, EuroISPA believes it is unlikely any resulting legislation will be practicable.

Recent Draft Framework Decision from France, Ireland, Sweden and the United Kingdom

The April 2004 proposal for a Council Framework Decision on data retention, submitted by four member states, was met with unified dismay from the EU's communication service providers (CSP) industry. The provisions place significant burdens on ISPs for the collection, storage and retrieval of data. When this is allied to the fact that it remains relatively unclear, due to the unrealistically broad terms in which the draft Decision is framed, which data fall within the scope of the proposal, it is no surprise that the text was met with such vociferous opposition. After the discussions of recent years, EuroISPA is extremely disappointed that such a proposal, which fails to take into account these discussions with industry, was tabled for high-level dialogue.

EuroISPA attended a meeting of the Forum for the Prevention of Organised Crime on 14 June 2004 with representatives from EU member states and the CSP industry. It is clear from this meeting, and our members' subsequent discussions in their own countries, that a wide divergence of opinion about the scope, retention period and many other details of the proposal, prevails between member states' governments. The authors of the draft Framework Decision understood this when drafting the text, which explains the numerous possibilities for derogation from certain aspects of the draft legislation and the lack of any precision in its technical aspects.

The European Commission specifies in its consultation paper that industry would prefer a closely harmonised approach to this issue across the European Union, rather than "a patchwork

[2] ECTA: European Competitive Telecommunications Association
ETNO: European Telecommunications Network Operators' Association
GSM Europe: European Interest Group of the GSM Association

of diverse technical and legal environments." There is some justification for this statement, but only insofar as legislation includes sensible and workable provisions in terms of the types of data concerned, the periods of data retention, the technical feasibility of any requirements and the costs. If the interests of all stakeholders are not taken fully into account, it seems unlikely that any subsequent texts will be an improvement on that which member states are scheduled to discuss in late September.

Current experience with regard to retained data raises a number of issues which are worth bearing in mind when formulating policy in this area. Firstly, different types of data are stored by ISPs for varying periods of time, with more specific data held for shorter periods. Even more problematic for developing a system that has the possibility to be useful for law enforcement authorities, log records are often in proprietary formats that are specific to the equipment or software using them, while raw log data may not even be machine-readable. Moreover, in line with data protection requirements, some of this data is automatically anonymised. In addition, one EuroISPA member association reported that many smaller ISPs have never received a request for data, while larger ISPs have only received a handful of requests.

Responses to the European Commission's questions

EuroISPA's responses to a number of the European Commission's questions illustrate the immense difficulties that data retention regimes present for ISPs. EuroISPA also emphasises how these burdens do not affect all ISPs in the same manner: the extent of the effects depends upon the size, service portfolios and network design of the ISP. Given the time constraints of this consultation period, we have concentrated on the illustration of important, general considerations that EuroISPA does not believe are currently appreciated by all stakeholders in the discussions.

Current Practices relating to data retention

- Current ISP practices of traffic data storage for business purposes, including how long the traffic data are stored, according to services concerned and types of offerings

Article 6 of Directive 2002/58/EC permits the storage of traffic data for as long as it is required for billing purposes. Article 6(5) contains wording that is interpreted in some EU member states as allowing the retention of some data for network security purposes. However, in each case, data must be deleted once it is no longer necessary for these purposes.

Nonetheless, compliance with Directive 2002/58/EC does not give rise to a situation whereby ISPs retain similar data for similar time periods. The differing nature of services provided by each ISP, the differences in their network structures and differences, therefore, in the types of

data they generate mean there is no period of retention for each data category that can be applied uniformly to the ISP industry.

Where it is consistent with data protection rules, there nevertheless appears to be a trend in some EU member states that Internet access providers retain access data (that is, which IP address was allocated to a subscriber on which access medium at a certain time) for three months for billing or network security purposes. However, this is certainly not a uniform trend. For example, some members report that broadband access providers, who do not require access data for billing purposes, delete access data immediately after the communication is completed. This raises questions regarding the feasibility of the principle in Recital 6 of the draft Framework Decision, which makes it clear that the proposal should be limited to "*certain types of data, which are already processed and stored for billing, commercial or other legitimate purposes".*

There are no consistent retention periods for application usage data (such as smtp, pop3, http, nntp and imap logs). Many ISPs do not retain such logs and, if they do, retention periods vary in accordance with their network security requirements.

Non-billing data, while being potentially useful for law enforcement authorities in isolated cases, would create vast stockpiles of unmanageable data were everything to be retained for law enforcement purposes. When we reflect that some member states stated in their reply to the 2002 Council questionnaire[3] on the subject of data retention that they felt that no further rules were needed, it is hard to imagine that such a measure is, in the words of the draft Framework Decision, "*strictly proportionate to the intended purpose*" - especially as the draft legislation makes it clear that the data is to be retained to investigate terrorism *and other offences*. In other words, the measure aims to have data retained for non-terrorism related purposes, for which it cannot be credibly argued that any new situations exist since the questionnaire was issued.

The infrastructure that needs to be created to ensure the retention, retrieval and handover procedures would be particularly burdensome for all ISPs. This would apply even to those smaller ISPs who would have to endure this cost in the knowledge that they have never received a single request for data.

- Current practices for public authorities to access and/or preserve the data stored, according to services concerned and types of offerings:

- the nature and the age of the data requested by law enforcement authorities;

EuroISPA members report that the majority of LEA requests for data relate to subscriber and access data. In other words, most requests seek to determine which subscriber was allocated

[3] Council of the EU Document 14107/02 (no longer available from the Council of the EU's website)

which IP number on which access medium at what time. EuroISPA members' experience is that the data retained for normal business purposes is fully adequate for law enforcement needs.

- the procedures to which such requests are submitted;

ISPs across the European Union report that their relationship with law enforcement authorities is extremely productive. Collaboration with LEAs to fulfill their lawful requests for access to certain data operates well, even though there are no mandatory ISP single point of contact (SPOC) schemes in place among the ISP industry. Larger ISPs have established their own SPOC in order to facilitate the receipt of requests from LEAs and ensure that response times are as low as possible. Indeed, EuroISPA members report that apart from certain court orders that specify timescales, there are no current legal requirements to respond to court orders or equivalent notices from LEAs within exact time periods (the exact format of notice differs between member states). ISPs have simply responded "as soon as possible", which clearly appears to be welcomed by LEAs. On the other hand, one member state has a quasi-mandatory LEA SPOC, which is an approach supported by ISPs in that country.

- if and how additional costs are taken into account or reimbursed;

Some EU member states have cost recovery systems for ISPs' responses to LEA requests. However, costs for additional technical infrastructure that must be installed to enable retention, in those countries where mandatory data retention systems have been put in place, are generally not reimbursed. France is the exception to this rule, where the law of November 2001 states that costs resulting from the mandatory storage of data will be reimbursed. There is no indication yet as to how or whether this law will be strictly implemented.

There is no cost recovery for requests to preserve data, though an ISP may later recover certain costs for its response to a court order to grant an LEA access to the data.

- Data Retention for law enforcement purposes at EU level:

- the technical feasibility of specific data retention requirements, in relation to the cost of data retention requirements in specific services or offerings.

<u>Technical feasibility</u>

It is clear that any data has the potential to be retained. However, the vast majority of data generated in the course of a communication has no reason to be retained and in many cases, the ISP has no current capability to retain that data.

When a legislator talks about the retention of certain data for a certain period of time, this can have very different implications for different ISPs. ISPs' networks are not identical; they are built according to their service offerings, technical developments and the evolution of the company. It is therefore extremely difficult to give an accurate overview of the technical difficulties for ISPs in complying with data retention obligations. Nevertheless, the following issues are representative of the majority of ISPs' concerns:

Data Collection:

Data is collected in various parts of an ISP's network. The vast majority of this data is not logged by any ISP, due to the lack of any purpose for it and its sheer volume.

Authentication data, IP assignments and flow logs are among the data collected in network elements such as routers and switches. Data logged in forwarding equipment will be in raw format and often incomplete. Thus information from an outside source, such as the DNS or an ISP, may be required to produce meaningful logs. Even if this isn't the case, raw data will need to be pre-processed if it is to be readable at a later date. Added to this is the consideration that the same data will be logged several times in the network, thus raising concerns about the duplication of data (see the box below on "Multiple data retention"). If data retention in line with the current draft EU Framework Decision is implemented, a conservative estimate is that ISPs would be forced to log anywhere between 50 and 100 times the data that is currently logged, depending on their network configurations.

Servers and service gateways log data for individual services. Though this is the largest potential source of communications data, there are numerous difficulties for ISPs in systematically logging this data. Log files do not have common formats - they are designed for humans and are not easily machine-readable. Depending on the log detail level, they can contain formidable amounts of data. It must also be considered that anonymous use of services, or use under a different user name, is often possible, while the source of most logs is actually the intermediary itself, for example through the use of load balancing or NAT. Therefore, much of this data would be irrelevant for any law enforcement investigation. Notwithstanding this, Article 6.e of the draft Decision places a requirement on ISPs to ensure the accuracy of all retained data including, by default, anonymised data for which no verification procedure can logically exist.

Multiple data retention

Some opponents of the draft Council Framework Decision have described its obligations as the equivalent of retaining a record of the sender and recipient of each letter that goes through the postal service. In reality, the proposals are far more cumbersome than even this rather worrying analogy. This is

because messages usually originate and terminate on different networks, possibly going through other networks *en route*. For a simple e-mail, there will be at least two essentially duplicate logs: one from the originating mail server and one from the terminating network.

With the development of convergence technologies, communications will travel through many more networks as consumers communicate across platforms in a way not previously possible. So, for example, it will be possible for a businessman to send an e-mail via Instant Messaging over a GPRS Internet connection while travelling abroad. This would generate, at the very least, logs concerning their connection and disconnection times to the foreign GPRS system, log on and log off times on their Instant Messaging connection, logs for the sending of the e-mail via their service provider's mail servers, logs for the receipt of the e-mail in the recipient's e-mail services and logs in the home GPRS network.

The proposal, as it currently stands, not only creates obligations for service providers to retain data they do not need and cannot legally use, it also creates obligations which *de facto* cause essentially identical data to be stored at multiple locations by multiple service providers and, having already caused CSPs considerable problems regarding the protection of personal data, places additional obligations on service providers to ensure that this data is kept securely.

Data Storage:

The actual storage of data presents a number of technical difficulties, considerations and costs for ISPs. Long-term (i.e. for a period of more than 30 days) storage of data is only practised where billing records must be kept for such periods by law; otherwise data protection rules require data to be deleted after short-term storage for billing or network security reasons.

A major technical consideration for long-term data retention is that the long-term secure storage of logs is not an industry standard practice. However, long-term storage of increased amounts of data will certainly require significant security measures to be taken, which implies a huge cost for all ISPs. The retention of such vast amounts of data increases considerably the risks of data spillage, leaks or even theft – creating security risks where previously none existed.

Any requirement for the long-term retention of data will mean that massive additional volumes of data must be kept. It is impossible to put figures on the exact increase in volumes and the costs thereby associated, because it will depend on the ISP's service portfolio, the number of subscribers and their consumption volume. Realistically, storage levels would be hundreds of times greater than today for small ISPs, if they had to comply with the broad provisions of the draft EU Framework Decision. Medium and large ISPs would need to multiply that figure considerably. While common storage media may not individually be hugely expensive, the storage devices that would be required to store such large volumes of data certainly would involve substantial cost: systems with the ability to store this data are simply not in use today.

As with data collection, data storage will need to be preceded by data processing, this time to correlate the data. This not only adds further cost to the process, but also raises significant concerns for ISPs in terms of their compliance with data protection regulations.

Data Retrieval:

There are immediate issues relating to internal resources to handle LEAs' requests for data, even if the number of requests does not increase. Retrieving requested data from such large storage volumes will increase the turn-around time. It is inevitable that ISPs would have to develop new retrieval systems to cope with the increased volumes of data.

In terms of know-how, ISPs' personnel for handling LEA requests must be extremely highly qualified staff. Even then, ISPs' internal technical systems change radically on a regular basis, since they must adapt to technological and service advances. Thus, ISPs will have to develop and maintain their own numerous data retrieval software, which is able to access recently stored logs and, with even greater difficulty, logs stored longer ago. Additionally, ISPs' staff turnover will pose serious problems, since it is almost impossible for the majority of ISPs to ensure adequate numbers of staff are sufficiently well trained to be able to work with complex and secure systems, set up by former technical staff, but which may no longer be fully in use.

It must be noted that data mining is an extremely complex task. Not only will it become increasingly difficult over time to guarantee the availability of data requested by LEAs, it will also become progressively more difficult to guarantee the quality and accuracy of data retrieved. Non-billing data is not of evidential quality, which means it might not mean what it first appears to signify.

Costs associated with data retrieval, taking into account increased levels of data for extended retention periods, will thus be colossal. The development, maintenance and staffing of retrieval systems implies considerable cost, while the cost of each retrieval will undoubtedly increase significantly from current levels.

- the financial implications of data retention

The sources of costs relating to data retention are highlighted above. However, it is impossible for EuroISPA to put any accurate cost assessments on the financial implications of data retention for ISPs in the European Union. We can state with certainty that the costs will be huge; but exact amounts depend on a number of factors including: the size of the ISP's network, number of subscribers, services offered, duration of retention regime, which data fall within the retention regime and quality of the data (i.e. must it be of evidential quality?). In addition, particularly for smaller ISPs, disproportionate costs are likely to arise - for example, regarding personnel for dealing with requests, attending court cases and maintaining "golden copies" of data passed over to law enforcement authorities.

Whatever the costs involved, discussions at national level, in which EuroISPA members have been involved, do not indicate any willingness by governments or law enforcement to cover all associated costs. It is thus inevitable that the cost to consumers of information society services will in turn be increased, at a time when governments and EU institutions are imploring ISPs to cut their prices to increase take-up and consumption of services. It has to be assumed that Europe will consolidate its position as the most expensive region for information society services.

Equally worrying for EuroISPA is that, since ISPs will suffer varying cost burdens from data retention regimes (for the reasons highlighted above), the competitive environment will be distorted. The financial implications of data retention are clearly significant enough for EuroISPA to be justifiably worried about the basic future of the European industry.

Conclusions

EuroISPA welcomes the European Commission's initiative for a consultation on issues relating to data retention. In this paper we have identified a number of features of existing frameworks for ISPs' collaboration with LEAs and underlined our significant concerns relating to proposals for extended data retention regimes. In summary, EuroISPA would like to stress a number of points from the ISP industry's perspective that must be fully considered before discussions to implement data retention proceed:

- Data protection and data retention requirements are almost mutually exclusive, thus putting ISPs in a genuinely impossible situation.

- Data processing and correlation of logs will be an activity carried out exclusively for law enforcement, since these are not normal procedures for ISPs.

- Logs are simply not designed for sophisticated access or long-term retention.

- To put ISPs' current practices into perspective, it must be noted that ISPs retain relatively less data as services develop. Broadband connections and a number of the services that run over them, such as email, are unmetered and therefore require less data for billing purposes. New services such as VoIP and video-related services will be only partially metered. Even so, a conservative estimate for a medium-sized ISP is that 65% of the data it currently retains is for legal rather than operational purposes. Data retention obligations will increase that figure drastically.

- Neither the introductory text to the draft Framework Decision, nor the presentations from member states at the 14 June 2004 meeting of the Forum for the Prevention of Organised

Crime, has outlined further guidance on the justification for long-term data retention. EuroISPA continues to be frustrated that very little evidence is ever provided for billing data being insufficient for law enforcement purposes, or to support the assertion that data preservation is inadequate. In particular, ISPs believe data preservation is a proportionate and efficient mechanism for law enforcement's requirements. Mandatory retention of traffic data is not only a potential infringement of *fundamental* rights, it also creates extraordinary costs and therefore requires – in order to be compliant with, *inter alia,* the requirements listed in Article 15 of Directive 2002/58/EC and highlighted in recital 7 of the draft Decision – the irrefutable need for the imposition of such a measure to be clearly demonstrated. Data preservation, on the other hand, does not raise the same problems either from a business or a civil liberties perspective, yet, from our experience, does give law enforcement authorities manageable and useful data.

- EuroISPA and its members are increasingly disturbed at LEAs' suggestions that data retention is required to compensate for inefficiencies in international cooperation and judicial processes.

- EuroISPA raises many points in this submission that question whether a blanket data retention regime would be of assistance to LEAs. Longer response times to LEA requests for data and the inability to guarantee the quality of the data would seem to defeat any justification put forward by LEAs in favour of data retention.

In conclusion, EuroISPA strongly urges the European Commission and EU member states to ensure that representatives of all parts of the communications service provider industry are involved in all discussions on any legislative proposals for data retention. If associations such as EuroISPA are not involved, there is little chance that any obligations will be practicable. Any obligations must balance the fundamental rights of data protection and the legitimate needs of law enforcement. EuroISPA therefore reiterates the need for a full impact assessment of proposed measures such as the draft Council Framework Decision.

About EuroISPA:

EuroISPA is the world's largest association of Internet Service Providers, representing around 800 ISPs across the EU. EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet. Its secretariat is located in Brussels.

EuroISPA is predominantly funded by its member and associate member associations and the members of the EuroISPA Industry Forum.

For further information on this and other matters concerning EuroISPA, please contact Richard Nash, Regulatory Affairs Manager and Secretary General, at the address set out below.

EuroISPA EEIG: Rue Montoyer 39, bte. 3, B – 1000 Brussels
Tel: +32 2 503 22 65 – Fax: +32 2 503 42 95 – secretariat@euroispa.org
http://www.euroispa.org