



– November 2004

## **Background Paper on Traffic Data Requirements and Cooperation with Law Enforcement Authorities**

### **Introduction**

WITSA has consistently urged governments to rely on the preservation rather than retention of communication data for law enforcement purposes. Data preservation orders would allow for specific data to be 'frozen' until law enforcement agents can access it using a legal warrant. Such orders would apply to all communications of a specific individual, device or address for a finite, specified period. This was in fact the investigative information gathering measure agreed upon in the Council of Europe Convention on Cybercrime.<sup>1</sup> "

Currently, the European Union is reviewing a draft Framework Decision<sup>2</sup> for communications data retention throughout Europe. According to the draft, EU member governments would require communications service providers – such as telecommunications companies, Internet service providers and other industries that provide related information services – to store information about every communication made by each of their customers. Given the breadth of retained information covered in the proposal, this would include storing the location data of mobile phones, lists of websites visited, all details of phone calls made including the caller and recipients and details of any emails and text messages sent. In addition, companies that temporarily retain individual customer information for billing and related business purposes would be required to keep it in a form accessible to law enforcement and other government

---

<sup>1</sup> See Council of Europe, Convention on Cybercrime (Budapest, 23.XI.2001), at Title 2, Article 16. Data preservation is also the preferred method for law enforcement investigative data gathering among several EU Member States (including Finland, Germany and Greece) and the United States.

<sup>2</sup> The full title is a "Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services," Council of the European Union, 8958/04 (Brussels, 28 April 2004).

agencies for variable ranges of one to three years, subject to member government discretion.

As the European Union and other governments review additional ways to protect communications, an open dialogue between governments and industry is paramount to ensure that law enforcement authorities get the support they need from communication providers while avoiding exorbitant technical and financial burdens on business. In this spirit, WITSA offers some specific commentary and recommendations.

### **World Information Technology and Services Alliance**

The World Information Technology and Services Alliance (WITSA) is a consortium of 65 information technology (IT) industry associations from economies around the world (list attached). As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information;
- providing members with a vast network of contacts in nearly every geographic region of the world; and
- hosting the World Congress on IT, the only industry sponsored global IT event.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including:

- increasing competition through open markets and regulatory reform;
- protecting intellectual property;
- reducing tariff and non-tariff trade barriers to IT goods and services; and safeguarding the viability and continued growth of the Internet and electronic commerce.

### **Traffic Data Requirements Should Contain Demonstrable Need and Proportionality**

In determining the appropriateness of traffic data requirements, WITSA sees at least three threshold questions:

- First, what information do authorities hope to retrieve, and what is the need for it?
- Second, what authority or process is necessary for service providers to provide data pursuant to law enforcement requests?
- And third, what is the impact on both individual rights and the economic viability of the service. And, how does this impact balance between the need for the information and the potential for its successful retrieval?

Service providers have a strong track record of working closely with law enforcement authorities (“LEAs”) under national statutory arrangements. Recent cases suggest that there is a good and sufficient co-operation between law enforcement and industry which involves data stored for less than 3-6 months. However, this will not always be the case as situations across countries and business models differ. Some member countries consider that data retention for 6 months inflicts substantial burden on industries. For example, in Japan, where data preservation law has just been established, data is retained for 3 months. This cooperation often includes real time interception of communications and the retention of traffic data that are routinely collected for legitimate business purposes. The current experiences of major service providers are:

- For voice services, the information typically sought includes:
  - identification of calling or called number (name, address, etc.);
  - duration of the call; and
  - characteristic of the subscription (flat rate, means of payment, etc.).
- For IP services, the information typically sought includes:
  - identification of a customer (name, address, age, etc.) and IP address; and
  - characteristic of the subscription (flat rate, means of payment, etc.).

At a minimum, any proposal should set a relevant traffic data definition that both reflects the current global state of communications networks and services *and* is flexible enough to assimilate the next generation of services. Industry would welcome consultation with policymakers to assist in suggesting an appropriate definition and/or to periodically review the appropriateness of a definition that is set.

In addition, any duration set by legislation should act as a ceiling – beyond which retention could not be required under law – and not set a suggested scope. Such a ceiling should first be supported by “demonstrable need” from LEAs. Only then can a duration ceiling be appropriately addressed with industry to determine whether it is proportionate” given the limited retention of current industry practices. As evidenced by current LEA needs, and a retention approach that balances the issue of privacy compliance, the maximum for this ceiling would likely be 3 months<sup>3</sup>.

In reviewing LEA needs and balancing it against both the privacy rights of individuals and industry capabilities, “proportionality” will also likely require the following:

- A cost reimbursement scheme is a necessary component to any retention framework, to cover the costs of retention and searching beyond business cases and to safeguard the privacy rights of individuals.

---

<sup>3</sup> Second Paragraph of Article 16 of the Convention of Cybercrime (Expedited preservation of stored computer data) clearly states: “the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, **up to a maximum of ninety days**, to enable the competent authorities to seek its disclosure.”

- Access to data retained should continue to be limited to law enforcement and for criminal investigative purposes only, under a clear process for an LEA to achieve the requisite authority.
- Waivers should be put in place for a service provider acting in conformance with a valid LEA request for access to retained data to protect service providers from liability to an end-user.

### **Traffic Data Requirements Should Take into Account the Impact on Industry, in particular financial implications and the technical feasibility**

WITSA does not support the establishment of a mandatory data retention policy for criminal investigation purposes. The storage and data retrieval costs attributable to mandatory retention are very high, are still being measured, and would increase significantly if a service provider is subject to variable retention requirements in different jurisdictions where it operates. The reasons the costs are continually being measured are simple. Even if a service provider does retain, for a minimal period, the traffic data an LEA may require, industry is not in the business of searching that information in a way that an LEA might desire. However, it is possible to isolate two primary factors that drive such costs:

- The cost to both store and search data stored from a network increases exponentially over time.
- The ability to effectively search retained bulk data decreases exponentially over the same period.

Further, certain costs can be borne by service providers from liability to an end-user for data retained and provided to an LEA. Service providers have a particular stake in assisting law enforcement to keep communications services secure. However, without clear rules governing what process is necessary from an LEA for access to retained information, users would be subjected to surveillance of their communications based upon varying levels of substantiation, further eroding consumer confidence. Without a warrant, order or similar due process control,<sup>4</sup> service providers would expose themselves to potential liability for the results of retention access requests, whether legitimate or not. To this end, key components of a balance with investigative aims must be the twin goals of process to protect communications end-users *and* immunity for intermediaries that follow the instructions of law enforcement.

Current industry storage practices differ widely among SMEs, major industry players, IP backbones, end-consumer business, traffic volumes and network architectures. Where such storage practices have developed, the retention times are driven by business requirements (*e.g.*, billing and related litigation, performance, security and maintenance of networks) and relevant data privacy requirements to purge the relevant data. Most

---

<sup>4</sup> The level of process necessary from an LEA should – and frequently does – track the level of risk for misuse attributable to particular type of information sought in an LEA request.

data stored, whether for voice, Internet or related value-added network traffic, generally reflect the following basic practices:

- The storage of “live” traffic and location data on servers is relatively short (2 days maximum).
- After two days, the data is transferred to tapes, which are held for various durations, generally dependent on the location of the server in question.
- This data is stored as ‘raw data,’ and does not include everything that a retention proposal might choose to define as “traffic” or “location” data.
- For instance, IP session data – details of web site browsing, as included in some retention proposals – would include billions of sessions every day.
- Networks are not designed to collect this data.

What is some of the ‘raw data’ that is stored? Again, practices among and within industries can widely differ, and the duration – although uniformly brief – will vary widely, but the below may be indicative for many:

	<b>Data to trace and identify communication source (contact inf., identity of service)</b>	<b>Data to identify the routing and destination of a communication</b>	<b>Data to identify the time, date and duration of a communication</b>	<b>Data to identify what type of device is used</b>	<b>Data to identify location throughout Communication duration</b>
Telephony providers	YES – but only current, not historical	YES	YES	YES	Mobile services only – not fixed
ISPs	Name, address etc.; log-on/off timing, and IP address (+CLI, if applicable)	For email: To:, CC:, and BCC:; e-mail header lines; IP address of destination domains, unless DNS changes are stored by another provider or spoofed FTP requests that lead to subsequent upload Screen Name of anyone sent file by IM NOT – routing or complete list of intervening routers – originating ISP cannot know this	Initiation and end of IM exchanges	Ethernet card USB modem Analogue modem	CLI should be sufficient as telcos can then identify user (need exemption if dialler software prevents CLI)

However, the above estimation of practices does not even begin to address the issues concerning the search of information that might be retained. Industry stores data in a limited fashion – primarily as raw data – in order to comply with business, privacy and

security requirements at minimum cost. Raw data, even if retained, requires data 'restoration' before it would become 'identifiable.'<sup>5</sup> Thus, any archived data would need to be first searched and then restored, if raw, which is likely the case. Depending on the duration of the request, and type of information requested, retrieval can be time consuming and costly even if the information is stored. Both effort and cost increase the longer back the request goes, as the continual evolution of technology requires not only the writing of software, but also knowledge of network storage patterns, practices and specific hardware. If the data exists, the time for retrieval and restoration can potentially be months.

### **Conclusion and Recommendations:**

WITSA has consistently recommended that governments utilize the preservation rather than retention of communication data for law enforcement purposes. .

An open dialogue between governments and industry is paramount to ensure that law enforcement authorities get the support they need from communication providers while avoiding exorbitant technical and financial burdens on business.

Inconsistent and disproportionately heavy traffic data requirements will drain limited resources without strengthening either the cooperative bond between law enforcement authorities and communication service providers or the investigative utility of information retrieved from such measures.

WITSA recommends:

- Governments to rely on data preservation as an alternative to the wide-scale, mandatory rules imposed by communications data retention.
- Any assessment of traffic data requirements must include certain criteria in order to be proportionately implemented and effective for its intended investigative purpose.<sup>6</sup>
- Governments should seek advice and opinions from key industry stakeholders before considering any proposed traffic data regime. Insufficient public input and lack of international harmonisation will result in policies that not only harm providers of communications services and their end-users but also impair the IT services market to citizens.

---

<sup>5</sup> The term 'identifiable' should be understood loosely in this context, for in the case of e-mail communications, customers can easily shift server usage, falsify addresses, and/or use relays to shield recipients, which will lessen the utility of information restored and 'identified'.

<sup>6</sup> *ICC Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes*, 4 June 2003, at [www.iccwbo.org/home/statements\\_rules/statements/2003/Common%20Industry%20Position%20on%20data%20retention%20final%20june%202003%20logos.pdf](http://www.iccwbo.org/home/statements_rules/statements/2003/Common%20Industry%20Position%20on%20data%20retention%20final%20june%202003%20logos.pdf).

- Policymakers should be mindful of the following:
  - The scope of requirements (*i.e.*, avoid overly broad definitions of traffic data and excessive storage periods);
  - Significant costs involved with storing and processing large volumes of data;
  - Technical feasibility (*i.e.*, understand how hardware and software modifications can or cannot accommodate data storage and processing requests);
  - Damage to end-user confidence, due to privacy concerns and increased security risks involved with storing large volumes of data; and