September 13, 2004

Hon. Fabio Colasanti
Director-General for Information Society
Directorate B.1: Communication services
Email: infso-b1@cec.eu.int

Hon. Jonathan Faull
Director-General for Justice and Home Affairs
Directorate D.2: Internal Security and Criminal Justice
Email: jai-eu-forum-organised-crime@cec.eu.int

European Commission
B-1049 Bruxelles / Europese Commissie - Belgium

Dear Messrs Colasanti and Faull:

In response to the 30 July 2004 Consultation Document on Traffic Data Retention (the "Consultation") from the Directorates-General for Information Society and Justice and Home Affairs, we are pleased to submit the following comments for your consideration. The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 400 corporate members throughout the U.S., and a global network of 60 countries' IT associations. Accordingly, the issue of data retention is of critical importance to our growing global membership.

Since the catastrophes of 9/11 and Madrid, industry has performed well to support and co-operate with law enforcement, and the industry remains committed to provide necessary assistance in future. However, inconsistent and disproportionately heavy retention 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. Therefore, we appreciate the questions raised by the Consultation and here summarize some of the answers addressed in the attached paper.

- ***What are the financial implications and technical feasibility of specific data retention requirements, and what do LEAs already request?***

There are ways in which retention can serve law enforcement needs while safeguarding the economic viability of and consumer confidence in telecommunications networks. Industry's track record of cooperation with Member State law enforcement authorities (LEAs) is a testament to this. Ongoing cooperation and recent cases (including Madrid) prove that there is a

Information Technology Association of America
1401 Wilson Blvd. - Suite 1100, Arlington, Virginia 22209-2318 ■ Phone: (703) 522-5055 Fax: (703) 525-2279

good and sufficient co-operation between law enforcement and industry which involves data stored for less than 3-6 months. Indeed, 98% percent of LEA retention requests are addressed with data only weeks or less old. All necessary data seems to be available. If the data of importance to LEAs is already available, where is the justification for 12-36 months or more?

Until such a case can be made by LEAs, requirements for 12 months and greater durations would violate Article 15(1) of the Directive on Privacy in Electronic Communications (2002/58/EC, the "2002 Directive") and Article 8 of the European Convention of Human Rights and Fundamental Freedoms. Proposed retention requirements that go far beyond that which LEAs have already demonstrated a need through practice neither "constitute an appropriate and proportionate measure within a democratic society," nor are they "necessary to safeguard" the national and public security-related interests articulated in the 2002 Directive.

Proportionality between interests of all stakeholders (industry, law enforcement, civil society) requires justification from law enforcement for mandatory increases in data storage. The Commission's Article 29 Data Protection Working Party has emphasized since September 2002 that retained information and the respective duration required must be driven by a "demonstrable need" in order to overcome data protection and related risks to security and individual rights. To-date, neither the authors of the 28 April 2002 draft Framework Decision nor LEAs generally have shown "demonstrable need" as a necessary prerequisite to understanding the costs to industry for further retention.

Storage and data retrieval costs attributable to mandatory retention are high, and are still being measured, for simple reasons. Even if a service provider does retain, for a minimal period, the traffic data an LEA may require, it is not in the business of searching that information in a way that an LEA might desire. Imagine, for example, that a postal service would have to make a copy of every single parcel, letter or postcard, in addition to all information on the movements of the individual postal courier, and store it for 12-36 months or greater.

Most data − whether for voice, Internet or related value-added network traffic − is stored 'live' on servers for a maximum of two days. After two days, the data is transferred to tapes that are held for various durations depending on the location of the server. This data does not include everything that a retention proposal might choose to define as "traffic" or "location" data. And further, this assessment of practices does not even begin to address 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 requires data 'restoration' before it would become 'identifiable.'

Not only do times for search and restore and related costs increase exponentially with the duration required, but also, network storage patterns, practices and specific hardware become critical issues. Knowledge of network and system design is perhaps the most troubling when you consider the vast differences among Member State durations and definitions for data to be retained. Most networks, servers, and their design – particularly for multinational service providers – do not operate their integrated international networks strictly based upon geographic boundaries. What constitutes "traffic data" in Belgium is likely stored – if it is stored – along with what constitutes "traffic data" in France. In turn, it is frequently impossible to engineer multiple retention times for that data.

- ***Is a common traffic data retention regime at EU level for law enforcement purposes needed?***

Yes. Any further legislation on the retention issue at the EU level should seek to harmonize between privacy and retention rules among the 25 Member States. The starting point for any legislation on retention for investigatory measures is the need for a harmonized approach to

prevent a patchwork of laws that will balkanize global communications networks. Lack of harmonization is already an increasing problem in the EU. Existing EU law delegates authority regarding scope and duration of data retained to the Member States. Pursuant to Articles of the 2002 Directive, Member States may legislate mandatory retention durations for "traffic data" and "location data" and set the appropriate definitional scope for either term. The 2002 Directive and prior legislation provide guidance on the scope of both terms, but Member States are not required to follow it in national implementation legislation. As a result, conflicting definitions of traffic data (and relevant services) are evidenced not only between Directives, but also among vastly different definitions at the Member State level.

Multiple Member States have implemented legislation directed specifically at setting mandatory duration requirements to retain data for law enforcement purposes. The scope and detail of relevant data covered varies greatly, and myriad durations not only differ across jurisdictions but also continue to be debated and passed. Among EU Member States, implemented (or proposed) durations vary from .25 to as much as 3 and 2-4 years. Further, for as many durations as have been implemented, there are also nearly as many variations on what the durational requirements mean for service providers. The draft Framework Decision of 28 April 2004 would only lead to exacerbate this situation for global and pan-European systems and network architectures with an even broader and more prolix definition and imposing unjustifiably long periods to retain.

- ***What types of data should be retained, and what time period should apply?***

At a minimum, any proposal should – first – 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. Current EU and Member State legislation generally use the concept of "traffic data" without adding clarity to which data are precisely covered by the term. Among emerging national rules, the "traffic data" definition typically includes information that is personally identifiable to a party engaging in electronic communications − whether voice, data or other value-added services − on a dynamic network. However, the distinction between content and signalling or billing data in the modern network environment is increasingly blurred. As suggested by ISPA Belgium in its January 2002 Position Paper on Retention of Traffic Data, such flexible definitions have been drafted by EuroISPA and others. Industry would welcome consultation with legislators to assist in drafting an appropriate definition and/or to periodically review the appropriateness of a definition that is set.

Second – any retention duration set by legislation should act as a ceiling − beyond which retention could not be required under Member State law − and not set a suggested scope, as presented in the draft Framework Decision. 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 (*e.g.*, Germany), the maximum for this ceiling would likely be 6 months. This process of drafting and deliberation would ensure an EU framework that is not only consistent with existing laws and related privacy requirements, but also, soften aberrational 2-4 year requirements to mirror a duration that has been justified by "demonstrable need," "proportionality" and industry practice.

In reviewing LEA needs and balancing it against both the privacy rights of individuals and industry capabilities, we believe that you will also find "proportionality" to also require the following:

- A pan-European 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.
- Access to data retained pursuant to any mandatory retention requirement 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.

ITAA is deeply concerned that the costs and technical difficulties associated with the retention and subsequent access to data mandated by the draft Framework Decision and similar proposals will severely damage user confidence in electronic communications and industry ability to provide related services. For this reason, mandatory data retention remains one of the key business-affecting issues faced by our telecommunications and Internet service provider industry members in Europe.

An open dialogue between governments and industry is paramount to ensure that law enforcement authorities continue get the support they need from communication providers while avoiding exorbitant technical and financial burdens on business. Therefore, we applaud the Directorates in soliciting comment under this Consultation. We realize that this discussion is only beginning – a proper impact assessment among experts is needed. Thus, we look forward toward a continuing dialogue with you on this issue toward a retention framework that addresses demonstrable needs of law enforcement with a proportionate safeguard of the communications industry and the rights of civil society.

Please feel free to contact me or my Senior Vice President for Global Affairs, Allen Miller, at amiller@itaa.org should you wish to discuss this matter, and thank you for your attention.

Sincerely,

Harris N. Miller
President

Attachment (1)

In response to the 30 July 2004 Consultation Document on Traffic Data Retention (the "Consultation") from the Directorates-General for Information Society and Justice and Home Affairs, we submit the following comments for your consideration. The text is divided into the following sub-issues, and many of the questions raised in the Consultation are addressed.

We look forward to the public forum on retention to be held in late September and hope that the Consultation and comments received result in a needed dialogue on this issue so critical to the communications industry and civil society. The public dialogue on this complex and critical issue will help ensure a sustainable approach to law enforcement assistance, resulting in appropriate technical and financial obligations, legal certainty and consumer confidence in network security.

I. Current Legal Support for Retention:

Existing EU law delegates authority regarding scope and duration of data retained to the Member States. Pursuant to Articles 2b and 2c of the Directive on Privacy in Electronic Communications (2002/58/EC, the "2002 Directive"), Member States may legislate mandatory retention[1] durations for "traffic data" and "location data" and set the appropriate definitional scope for either term. Although the 2002 Directive and prior legislation provide guidance on the scope of both terms, not only does this guidance at-times conflict, but also, Member States are not required to follow it in national implementation legislation.

The 2002 Directive addresses privacy in the context of Internet and other value-added services that may be provided over a telecommunications network, whereas the requirements of the Directive on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (97/66/EC, the "1997 Directive") are limited to basic telecommunications services. Article 6(1) of the 1997 Directive defines "traffic data" as "data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network." In addition, the Annex to the 1997 Directive provides greater detail on the "traffic data" that can be acceptably processed in the provision of telecommunications services:

- number or identification of the subscriber station,
- address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,

[1] Data retention is the collection of all data traversing the network, regardless of sender/recipient or investigative purpose, for eventual review by authorities as need arises. Data retention proposals vary according to the type of data to be retained ("traffic," "location," etc.) and the duration for its retention.

- type, starting time and duration of the calls made and/or the data volume transmitted,
- date of the call/service,
- other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.

"Traffic data" as addressed in Recital 15 of the 2002 Directive is very different, owing to the Directive's broader electronic communications emphasis:

> Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, *inter alia*, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

This recital description of traffic data is refined in a succinct definition at Article 2(b): "'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". In addition, Article 2(c) of the 2002 Directive also specifically defines "location data," whereas the 1997 Directive does not: "'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

Apart from greater definitional detail, Article 15(1) of the 2002 Directive also provides that such "national diverging measures" as mandatory data retention are exempt from data protection rules (namely, to the "confidentiality of communications, limitations on the processing of traffic and location data and withholding of calling line identification"), so long as these Member State rules:

a) are based on national legislative acts (*e.g.*, restrictions cannot be based on voluntary agreements or on ministerial guidelines etc.);
b) are necessary to safeguard national security, defence, public security or are necessary for the investigation or prevention of crime or of unauthorized use of electronic communication systems (*e.g.*, general tax purposes are not an acceptable ground for restrictions in this context); and
c) constitute an appropriate and proportionate measure within a democratic society.

Exemption would apply equally to relevant principles under the Data Protection Directive (95/46/EC, the "1995 Directive"), the 1997 Directive, the privacy-related provisions of the 2002 Directive itself and national laws implementing each of the above. The criteria for derogation from data protection rules are directly derived from case law established by the European Court of Human Rights in respect of Article 8 of the European Convention of Human Rights and Fundamental Freedoms, which forms the basis of EU data protection and privacy legislation. In its response to frequently asked questions on the derogation, the European Commission has noted that "in its case law, the Court in Strasbourg has generally

taken a restrictive line on national measures deviating from fundamental rights and freedoms."

Further, Member State legislatures continue to increase technical interception[2] requirements for telecommunication service providers in a post-9/11 world. Thus, EU Member States can each set different requirements for the interception of data and its retention for investigative purposes. However, those countries that have already imposed mandatory data retention regimes require that the data be accessible only to law enforcement and solely for the purpose of criminal or tax investigations. None of the present proposals for mandatory retention even hint at providing access for private rights of action or infringement.

A. Draft Framework Decision:

Subsequent to full implementation of the 2002 Directive in October 2003, four Member States of the Council of the EU presented a draft Framework Decision[3] for communications data retention throughout Europe. This draft on mandatory data retention was jointly introduced by the justice ministries of France, Ireland, Sweden and the United Kingdom on 28 April 2004. The draft was completed within a European Council working group after the March 2004 Madrid terrorist attacks without any public debate, consultation with industry experts or coordination with other ministries responsible for the impacted industries. Its text was made public in late May 2004.

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

In addition to the lack of proper consultation with industry, there are specific fundamental concerns with much of the draft text. Most troubling, the draft requires mandatory data retention for a period of up to 36 months – or greater, if required under local law – equalling the longest duration presently prescribed in Member State law. This dangerously fails to recognize or consider industry's technological or financial capability to support durations that fall beyond the scope of existing business practices, which is typically of a far shorter duration.

Further, the defined data to be retained includes everything normally referred to as "traffic data," as well as broader sets of data such as FTP logs and website access logs. From the

[2] By court order or similar form of due process control, ISPs and other telecommunications providers can be required to perform data interception, the capture and collection of specific communications for a time-limited and specific investigative purpose.

[3] 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).

breadth of the current text, and particularly Article 2, it is exceedingly difficult to determine where the list of covered data ends. In addition to the breadth and vague nature of the definition, there are no provisions relating to cost recovery, despite that the draft contains multiple obligations on industry regarding retention durations far beyond any sustainable business cases. Further, service providers would be held to concomitant data protection requirements as to the quality of, security for and accessibility to data requested by law enforcement.

Finally, the recitals affirm, without any apparent justification, that the proposal does not infringe international rules with regard to the privacy and security of information, such as those embodied in the European Convention on Human Rights. The proposal states that retained data must be subject to the 1995 Directive, including obligations as to the confidentiality, integrity and accuracy of data retained. And yet, counter to data protection requirements, the data in question is mandated to be retained by industry for purposes unrelated to its collection and for durations beyond present business cases or needs. This extensive retention can be construed readily to be disproportionate and to create data privacy security risks.

The European Parliament could not have considered the draft prior to the conclusion of its session during the week of 9 May 2004, although its powers to amend proposals that fall under 3rd Pillar (cooperation on justice and home affairs) competency are limited. Article 8 of the draft Framework Decision stipulates that Member States will have two years for implementation. In addition, the EU Council Declaration on Combating Terrorism, dated 25 March 2004, states that all proposals on data retention should be concluded by the end of June 2005. A current projection based upon the recommendations of both documents would suggest that EU Member States will be obliged to implement mandatory data retention schemes no later than the summer of 2007.

B. Member State Laws:

Prior to and since passage of the 2002 Directive, multiple Member States have implemented legislation directed specifically at setting mandatory duration requirements to retain data for law enforcement purposes. Among these emerging national rules, the definition of "traffic data" is typically inclusive of information that is personally identifiable to a party engaging in electronic communications on a dynamic network − whether voice, data or other value-added services. However, the scope and detail of relevant data covered varies greatly among current and prospective national laws on retention.

For instance in France, Article 10 of the Law 2004-669 on "electronic communications" has now replaced Article 29 of its Law 2001-1062 on "daily security" to *require* retention where it had otherwise been permitted for business purposes. In contrast to other national laws, France has chosen to set a one-year maximum for retention. In other words, the list of applicable data to be retained for law enforcement purposes should be retained for up to one year and thereafter purged for purposes of data protection compliance. Greater detail on what "traffic" and "location" data should be retained is expected in a forthcoming governmental decree to implement the retention provisions of the "electronic communications" law. However, in lieu of the decree expected in fall 2004, subsequent consultations on Laws 2004-669 and 2001-1062 have provided detail on what is expected to be retained:

Internet: Customer address; user login; email address; billing addresses; connect data to the called terminals; complementary services which are Requested or used; the calling party number; any piece of information which shows the trunk ID and the switch ID; the called party number; date and time of start and end of connection; IP address from sender/user; sent and received email headers and SMTP; information on connection to Proxies; connection data to the called terminals; information related to the terminal of the caller. In addition, data related to the visiting of websites (pursuant to the law of March 18, 2003).

Voice: Customer address; date and time of start and end of communication; type of communication and technical characteristics (such as ingoing and outgoing calls, voice, data); the calling party number; location of the call; the called party number; complementary services (call forwarding, re-routing, etc); any piece of information which shows the trunk ID and the switch ID.

Data (leased lines): Customer address; origin and the type of circuit; date and time of start and end of communication; type of communication (and technical characteristics such as: ingoing and outgoing calls, voice, data, connection data to the called terminals, and Information related to the terminal of the caller).[4]

By contrast, consider the Belgian Telecommunication Law of 21 March 1991 and the Royal Decree of 9 January 2003 (implementing changes both to the Telecommunication Law and Criminal Procedure Code, articles 46bis, 88bis, 90ter). Pursuant to Telecommunications Law Articles 105 and 109, providers may keep traffic data necessary for billing purposes and fraud prevention, including:

- Number and address of the subscriber;
- the amount of unit to bill;
- called party numbers;
- date, starting and ending hour and duration of each call and or the amount of data transmitted; and
- information related to payments (payment by instalments, prepayments).

In turn, the Royal Decree addresses data to be retained for law enforcement purposes as:

- IP address (fixed or temporarily allocated).
- For dial connections: number of the caller; volume of data (incoming and outgoing); date (day, month, year) starting and ending hour and duration.
- For all other kind of connection: identification of the user and location of the connection to the Internet access provider.

As above, for some EU jurisdictions that have addressed the issue of mandatory retention, the protection of subscriber privacy is addressed in different legislation and with varying definitions of "traffic data." The *authority* to retain certain data – for business purposes – may differ greatly in scope from a separate *requirement* to retain for law enforcement

[4] The 2002 Directive was implemented following passage of France's Law 2001-1062, but subsequent consultations on the forthcoming decree still cite the "traffic data" definition of the 1997 Directive. As many comments have pointed out, this definition does not take into account the evolution of communications and various value-added services that the scope of the decree would purport to address.

purposes within a given jurisdiction. Not only do definitions often vary within country, for protection of rights and law enforcement purposes, respectively, but also – and of significant concern to service providers – the "traffic data" to be retained for law enforcement purposes varies greatly from Member State to Member State, as evidenced by France and Belgium.

These myriad durations not only differ across jurisdictions but also continue to be debated and passed. The most recent mandatory duration passed – that for Italy, in late February 2004 – set a duration of two to four years, the longest to-date in the EU. The below chart depicts mandatory retention durations implemented (or proposed) in several EU Member States. Further, for as many durations as have been implemented, there are also nearly as many variations on what the durational requirements mean for service providers (as depicted in the below notes).

EU Member States +	Mandatory Retention Required (in years)
Austria	0
Belgium	1
Denmark	1
Finland	.25 *
France	1 †
Germany	0.5 ‡
Greece	0
Ireland	3 ♠
Italy	2-4 **
Luxembourg	0
Netherlands	.25
Norway	0
Portugal	0
Spain	1 ††
Sweden	1 ♠
Switzerland	0.5
United Kingdom	1 ‡‡

* Minimum of 3 months / maximum of 3 years is pursuant to Protection of Privacy and Data Security in Telecommunications (723/1999) Act and not mandatory retention for law enforcement purposes.

† One year is a maximum, subject to forthcoming decree.

‡ Not a mandatory minimum, but a maximum period allowed for the retention of user-related accounting data unless there are payment disputes.

♠ Proposed, but not yet enacted.

** Minimum of 24 months required. Under certain conditions, a court can order that the traffic data must be stored for another 24 months. ISP email traffic data is excluded from the provision.

†† Subject to additional forthcoming legislation.

‡‡ A voluntary program, at present.

II. Government, Association and Industry Expert Commentary:

This fractured result − multiple definitions and varied national durations – was lobbied against heavily through 2004 by global NGOs, industry associations, academic and technical

advisors, and government officials. In 2003, global industry participated in a coalition with the International Chamber of Commerce ("ICC") and global representative associations – including the Union of Industrial and Employers' Confederations of Europe, the European Information and Communication Technology Association, the International Telecommunications Users Group and ITAA – that urged governments to consider data preservation as an alternative to the wide-scale, mandatory rules imposed by communications data retention. Data preservation allows for specific data to be 'frozen' until law enforcement agents can access it using a legal warrant.[5] Most nearly like a traditional wiretap, with preservation authorities require retention of all communications but only for a specific individual and for a finite period specified in an order. This was in fact the investigative information gathering measure agreed upon in the Council of Europe Convention on Cybercrime.[6]

However, the ICC position that resulted from the coalition also emphasized that mandatory retention, where legislated, would need to embody certain criteria in order to be proportionately implemented and effective for its intended investigative purpose.[7] The coalition urged governments to co-ordinate toward a data retention regime based on advice and opinions from key industry stakeholders. Insufficient public input and lack of multi-lateral 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 the detriment of all European citizens. Paramount among the coalition's recommendations are for legislators to 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); and
- Damage to end-user confidence, due to privacy concerns and increased security risks involved with storing large volumes of data.

It is this first principle that was key to the ISPA Belgium's January 2002 Position Paper on Retention of Traffic Data. ISPA Belgium noted that, while its national retention requirement was a 12 month minimum, most other Member States at the time required a period of 3

---

[5] Since 9/11, the US government has maintained that retention is unnecessary to its terrorism-related investigative needs.

> "Investigators and prosecutors need the ability to have service providers preserve, for a limited period of time, data that already exists within their network architecture and that relates to a specific investigation. With respect to service providers choosing to retain data, the United States and other nations have taken an approach that neither requires the destruction of critical information nor mandates the general collection and retention of such data. Rather, service providers are permitted to retain or destroy the records they generate based upon individual assessments of resources, architectural limitations, security and other business needs."

E.g., Comments of US Govt. on "Network and Information Security: Proposal for a European Policy Approach" (COM 2001 (298)), at 9; Prepared Statement of US Govt. at the EU Forum on Cybercrime (Brussels, 27 Nov. 2001).

[6] *See* Council of Europe, Convention on Cybercrime (Budapest, 23.XI.2001), at Title 2, Article 16.

[7] *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.

months or less. "The divergent requirements in this respect, even between the EU Member States, are a serious obstacle for the development of European-wide network services and may restrict competition."[8] Moreover, as early as January 2002, ISPA Belgium foresaw that emerging EU and national definitions of "traffic data" were neither cognisant of swiftly developing services, nor specific enough for service providers to understand what to retain:

> Current legislation in this area generally uses the concept of "traffic data" without making it clear which data are precisely covered by this term. In the context of a traditional telephone network the distinction between content data and signalling or billing data was more or less easy to make but in the modern network environment the separation is progressively blurred. There are currently hundreds of different network services and the term "traffic data" is no longer appropriate to express the richness of data types involved in this new environment. ISPA pleads for clear definitions in this field such as those used by EuroISPA.

The ICC, ISPA Belgium, and many others also expressed great concern regarding the possible negative effect of data retention requirements on the adoption of network use by end-users. The continued development of a modern Information Society depends primarily on trust. This trust is critical to end-users in their use of networks for activities that they would otherwise typically perform offline. Thus, any disproportionate move away from the basic principles of data protection law should be considered as a serious threat to the consumer confidence.

Echoing ISPA Belgium and others, the European Commission's Article 29 Data Protection Working Party has expressed similar concerns. Following the 9 September 2002 meeting of European data protection commissioners in Cardiff, the Working Party reaffirmed that any proscribed retention period should be "as short as possible," and in any event, "less than 12 months" in duration.[9] The Working Party complemented this decision on 29 January 2003 by stating that "traffic data," the target for mandatory retention in several emerging Member State laws, should be required for no more than 3 to 6 Months (for "traffic data" already retained by industry for billing purposes).[10] Both statements by the Working Party emphasized that retained information and the respective duration required should be driven by a "demonstrable need" in order to overcome data protection and related risks to security and individual rights. This emphatic recommendation to implement a proportionate and limited approach was entirely lost in the April draft Framework Decision.

These and other senior national experts have repeatedly cautioned EU officials on the legality of traffic data retention mandates of greater than twelve months. Thus, it was extraordinary to learn that some European Council members are calling on industry to retain traffic data for up to three years under the draft Framework Decision. It is also striking that two of the countries proposing this measure (Sweden and Ireland) stated in 2002 that they saw no clear need for retention of information beyond existing industry business practices.

---

[8] ISPA Belgium: Position Paper on Traffic Data Retention, Jan. 2002, at 2.

[9] *See* Statement of the European DP Commissioners at the Int'l Conference at Cardiff, 9-11 Sept. 2002, on the Mandatory Systematic Retention of Telecommunications Traffic Data *and* Op. 5/2002, Art. 29 DP Working Party (11818/02/EN).

[10] Op. 1/2003 on the Storage of Traffic Data for Billing Purposes, Art. 29 DP Working Party (12054/02/EN), at 4.2.

For its part, the UK, also among the drafters, had reported that it was still too early to discern the effectiveness of its own voluntary code on data retention. Days before the text of draft Framework Decision was released, Home Office Minister Caroline Flint reported, in a Ministerial Statement of 14 May 2004, that "it will be possible to conduct a more thorough evaluation of the effectiveness of the Code" once service providers are given adequate time to retain data in compliance with it. The UK voluntary Code requires retention for up to 12 months,[11] whereas the draft Framework Decision suggests up to 3 years. These contemporaneous inconsistencies undermine arguments that more onerous retention periods are essential and highlight the need for a uniform and proportionate approach.

III. Demonstrable Need and Proportionality – First:

Several of the questions raised in the Consultation notice parallel the twin issues of "proportionality" and "demonstrable need" which were raised in the 2002 Directive and by the Working Party, respectively, in addressing the justification needed from law enforcement to expand retention requirements. These questions include:

- ***What are the current practices for public authorities to access and/or preserve the data stored, according to services concerned, and in particular:***
  - ***the nature and the age of the data requested by law enforcement authorities;***
  - ***the number and frequency of requests for given types of data;***
  - ***the procedures to which such requests are submitted;***
  - ***if and how additional costs are taken into account or reimbursed; and***
  - ***the effectiveness of current access regimes?***

In addressing these questions, we will take up the twin justification issues as well. Key to determining the appropriateness of retention requirements are 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 retained data pursuant to law enforcement requests?
- And third, what is the impact of retention 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. This cooperation often includes real time interception of communications and the retention of traffic data that are routinely collected for legitimate business purposes. Thus, the first key question above can be answered by the existing track record of telecommunications and Internet service provider ("ISP") industry assistance to law enforcement on retention requests. For instance, from the current experiences of major service providers among EU Member States, the following can be drawn:

[11] Retention of Communications Data (Code of Practice) Order 2003 (SI 2003/N0.3175) (5 December 2003).

- Roughly 98% of requests from LEAs for information targeted only the most recent few weeks of retained data.
- The remaining 2% consisted of requests from LEAs for information from no earlier than 6 months of retained data.
- Only 2 cases in five years were reported where an LEA expressed a need for information retained during a period greater than 6 months prior to the request (but less than a year).
- One of those requests – for 12 months, by the UK – was dropped after the service provider compiled the costs necessary for that specific search.[12]
- 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.).

Most LEA requests for access to certain retained information come from the state or local police of a Member State. In France, for purposes of example, the number of requests to a major services provider for basic voice-related telecommunications retained data typically amounts to between ten and twenty per week. Similarly for France, requests for IP-related retained data typically number 2-4 per month. Such requests seldom are made by administrative enforcement bodies.

Given that the data of importance to LEAs is already available, where is the justification for more extensive retention? Recent cases (including Madrid) prove that there is a good and sufficient co-operation between law enforcement and industry which involves data stored for less than 3-6 months. All necessary data seems to be available. Where is the business case for 12-36 months? To-date, neither the drafters of the draft Framework Decision nor LEAs generally have provided any evidence that more is needed.

Until such a case can be made conclusively by LEAs, requirements for retention of 12 months and greater durations would violate Article 15(1) of the 2002 Directive and Article 8 of the European Convention of Human Rights and Fundamental Freedoms. Proposed retention requirements that go far beyond that which LEAs have already demonstrated a need through practice neither "constitute an appropriate and proportionate measure within a democratic society," nor are they "necessary to safeguard" the national and public security-related interests articulated in the 2002 Directive. Proportionality between interests of all stakeholders (industry, law enforcement, civil society) requires justification from law enforcement for mandatory increases in data storage. The requisite "demonstrable need" for such increases has not been shown.

IV. The Impact on Industry – Second:

Several of the questions raised in the Consultation also seek comment on the impact to industry from retention. The questions are closely aligned to technical feasibility issues and

[12] Cost recovery is provided under an SLA with law enforcement, pursuant to the UK voluntary code.

related costs to industry in attempting to meet current and prospective retention requirements. These questions include:

- ***What are the current practices of traffic data storage for business purposes, including how long the traffic data are stored, according to:***
  - ***services concerned; and***
  - ***types of offerings?***

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. It is also for this reason that industry would see no business value in retaining data for the lengthy durations proposed in the draft Framework Decision. 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.

Consider, for Internet services for instance, that roughly 40 percent of most Internet email traffic consists of spam – and that this material would be retained as well – and you get one perspective on the potential storage and search problems.

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. It is for this reason that policy makers in Great Britain and France, among others, have taken particular pains to debate the quality and specificity of substantiation necessary to access personal information retained, particularly in the Internet environment. Without a warrant, order or similar due process control,[13] 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 data stored, whether for

[13] 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.

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.
- Retention of IP session data for the UK alone would crash most major networks within 2 hours if it was required to be retained.

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:

	Data to trace and identify communication source (contact inf., identity of service)	**Data to identify the routing and destination of a communication**	**Data to identify the time, date and duration of a communication**	**Data to identify what type of device is used**	**Data to identify location throughout Communication duration**
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.'[14] 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.

This last element, knowledge of network and system design, is perhaps the most troubling when you consider the vast differences among Member State durations and definitions for data to be retained. Most networks, servers, and their design – particularly for multinational service providers – do not operate their integrated international networks strictly based upon geographic boundaries. What constitutes "traffic data" in Belgium is likely stored – if it is stored – along with what constitutes "traffic data" in France. In turn, it is frequently technically impossible to engineer multiple retention times for that data.

In view of the above, the duration and scope of retention contemplated under the draft Framework Decision would require industry to create "server farms" (additional machines, per country of operation, to provide for the storage, analysis and retrieval of data according to separate and lengthy requirements). Not only would the creation of server farms be cost prohibitive and irrespective of business plans, but the negative impact on the speed, performance and security of a network operating with them would be immediate. Imagine, for example, that a postal service would have to make a copy of every single parcel, letter or postcard, in addition to all information on the movements of the individual postal courier, and store it for 12-36 months or greater. In turn, this does not even begin to address the costs and practical issues that would be attributable to secure such farms of pooled data pursuant to data protection rules. Nor does it address the critical information security risks that inevitably emerge if vast amounts of data are retained on a diffused basis. As drafted, the Framework Decision would lead to a disproportionate increase in resources spent, immediate performance impact to services, legal uncertainty and significant risks to data privacy and consumer confidence.

V. Conclusion:

Multinational communication industries support and continue to assist LEA efforts to fight crime and terrorism in a legally compliant way. However, inconsistent and disproportionately heavy retention 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.

Some may assert that, solely from a pure law enforcement perspective, complete and permanent surveillance of all citizens is the ideal solution to avoid criminality and terrorism. Such a solution is however totally incompatible with the basic principles of a democratic society. A democracy cannot function if it doesn't guarantee a sufficiently protected private sphere for every individual. Protection against crime and terrorism must never undermine the

[14] 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'.

essential characteristics of the democracy itself. Since the catastrophes of 9/11 and Madrid, industry has performed well to support and co-operate law enforcement, and the industry remains committed to provide necessary assistance in future.

Data storage requirements should not exceed what is necessary to achieve law enforcement objectives. We are deeply concerned that the extreme costs and technical difficulties associated with the retention and subsequent access to data mandated by the draft Framework Decision and similar proposals will severely damage user confidence in electronic communications and industry ability to provide related services. For this reason, mandatory data retention remains one of the key business-affecting issues faced by the telecom and ISP industries in Europe. LEA officials, including the parties responsible for the draft Framework Decision, have failed to describe how proposed retention durations will or can increase investigative effectiveness, crime prevention or anti-terrorism efforts. By contrast, the track record of service provider response to LEA requests does not show a need for either the durations recommended or the broad qualities of data suggested. We need to fight terrorism and serious crime, but not by crippling the communications sector with cost-prohibitive mandates and critically damaging public confidence.

- ***Is a common traffic data retention regime at EU level for law enforcement purposes needed?***

Yes. Any further legislation on the retention issue on the EU level should seek to harmonise between privacy and retention rules among the 25 Member States. Lack of harmonisation is already an increasing problem in the EU. As discussed above, the conflicting definitions of traffic data (and relevant services) are evidenced not only between the 1997 and 2002 Directives, but also among vastly different definitions at the Member State level.

There are ways in which retention can serve law enforcement needs while safeguarding the economic viability of and consumer confidence in telecommunications networks. Industry's track record of cooperation with LEAs in several Member States is a testament to this. The starting point for any legislation on retention for investigatory measures is the need for a harmonised approach to prevent a patchwork of laws that will balkanize global communications networks. Industry has been placed in a position to retain different types of "traffic data," within different Member State borders, often with systems and networks that have no capacity to engineer such restrictions according to geographic borders. The draft Framework Decision would only lead to exacerbate this situation for global and pan-European systems and network architectures by stipulating an even broader and more prolix definition and imposing unjustifiably long periods to retain.

- ***What types of data that should be retained by operators for each service?***
- ***And, what period of time should apply, according to the services and to the data concerned?***

At a minimum, any proposal should – first – 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. As raised by ISPA Belgium, such traffic data definitions have been drafted by EuroISPA and others. Industry would welcome consultation with legislators to assist in drafting an appropriate definition and/or to periodically review the appropriateness of a definition that is set.

Second – any retention duration set by legislation should act as a ceiling, beyond which retention could not be required under Member State law, and not set a suggested scope,. Such a ceiling should first be supported by "demonstrable need" from LEAs. Only then can the 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 (*e.g.*, Germany), the maximum for this ceiling would likely be 6 months. This process of drafting and deliberation would ensure an EU framework that is not only consistent with existing laws and related privacy requirements, but also, soften aberrational rules (Italy's 2-4 year provision) to mirror a duration that has been justified by "demonstrable need," "proportionality" and industry practice.

- ***What are the financial implications of data retention?***
- ***And, what is the technical feasibility of specific data retention requirements, in relation to the cost of data retention requirements in specific services or offerings?***

As discussed above, the myriad current definitions and durations among Member States require service providers to engage in retention in a manner for which their business and technology is largely unfit. The costs to these requirements are great, and under the draft Framework Decision, the costs attributable to "server farms" that would be necessary for compliance would nearly equate to the start-up costs of a new industry in and of itself. Such a retention scheme and duration could possibly warrant having a third-party ownership of the necessary equipment and processes.

The telecommunications and ISP industries are acutely sensitive to the need to safeguard European and national security interests. Further, we recognize that no one industry should bear the burden of implementing desired investigative mechanisms without either its consultation or consent. At the very least, industry needs a pan-European cost reimbursement scheme as a component of any retention framework. The UK recognized such a need in implementing its current voluntary retention program which reimburses carriers for the retrieval costs related to an LEA request. In at least one case, the disproportionate cost attributed to a lengthy search duration drove an LEA to re-think an investigative request.

Any proposed legislation should provide for cost reimbursement, even under circumstances where existing business practices might result in needed data being retained. Without a mechanism for equipment and human resource reimbursement, the cost burden of complex technical search, restore and retrieval could put service providers at substantial financial risk. Additionally, there will be a resulting opportunity cost in having to divert resources and technical expertise from further development and improvement of services. This, in turn, leads to both higher cost services and decreased availability of innovative services to the public.

Reimbursement would also serve to safeguard the privacy rights of individuals. If LEAs are held accountable for the costs of interception and investigation, it is likely that they will be deterred from abusing investigative requests, seeking over-inclusive requests or targeting individuals inappropriately. Because (in practice) the requests of LEAs often target a specific individual for retention or monitoring of their communications – and for a limited and finite

period of time – cost implications can be minimized and rights consequences brought within the margins of existing protections. The probability that a crime or violation is occurring is known, and the investigation limits clear. The protection of industry and fundamental human rights are uniquely linked in this application of economically rational cost/benefit analysis.

Access to data retained pursuant to any mandatory retention requirement 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. Further, to protect service providers from liability to an end-user, waivers should be put in place for a service provider acting in conformance with a valid LEA request for access to retained data. Such a waiver would serve to protect a service provider in fulfilling and LEA request, while recognizing its obligation to an end-user under data protection rules.

We urge the European Council to withhold the current draft Framework Decision, review the recommendations of the ICC coalition and related positions, and engage industry and privacy experts for an impact assessment to assure the proportionality and effectiveness of this and any future EU legislation on retention. Our members and colleague organizations are acutely sensitive to the need to safeguard European and national security interests. Further, we recognize that no one industry should bear the burden of implementing desired safeguards for the benefit of law enforcement and civil society.

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. Therefore, we applaud the Directorates in soliciting comment under this Consultation. We realize that this discussion is only beginning – a proper impact assessment among experts is needed. Thus, we look forward toward a continuing dialogue with you on this issue toward a retention framework that addresses demonstrable needs of law enforcement with a proportionate safeguard of the communications industry and the rights of civil society.