ITAA COMMENTS
On the 27 July 2005 European Commission
Interservice Consultation Proposal
For a
Data Retention Directive

In response to the 27 July 2005 release of the European Commission's interservice consultation proposal for a "Directive on retention of data processed in connection with the provision of public electronic communication services," and the late July release by the U.K. Presidency of a revised Council of Minister's draft Framework Decision, 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.[1]

ITAA and its members have therefore taken great interest in Europe's debate of mandatory retention measures. This debate has included the release of several draft Framework Decisions by the Council since April 2004 and the most recent effort by Commissioners to broker a compromise proposal in the form of the EC's draft Directive. We greatly respect the hard work and consideration of industry concerns taken by members of the Council, EC and European Parliament in this process. And further, we recognize that the most recent terrorist events and threats in London have elevated both the retention issue and the drive for a Europe-wide legislated framework to a fevered urgency. Like the UK Presidency of the EU, we encourage the legislative goal of increasing the investigative effectiveness of measures to combat terrorism. Thus, in the hope of adding to the substance of debate on existing drafts and the effectiveness of resulting measures, we submit the following eight-point executive summary and discussion below.

Executive Summary

1) Since the catastrophes of 9/11 and Madrid, and through recent terrorist atrocities in London, the communications industry has shaped a positive experience of co-operation with law enforcement agencies (LEAs) toward the use of communications-related information to investigate criminal activity.

[1] For more information about the ITAA and its members, please visit us at: www.itaa.org.

(a) This cooperative experience has affirmed that data retention according to present industry business practices is effective to advance the desired result: to provide effective means to combat terrorism.

2) Through release of several draft Framework Decisions since last April, the Council of Ministers has thus far not provided any sound evidence that:

(a) some providers are failing to engage in the minimum retentions required under their own business cases;

(b) that present business practices themselves are insufficient; or

(c) that LEAs have shown any demonstrable need for the retention described.

3) An EU harmonization measure – blending the most acceptable components of the Council and European Commission (EC) drafts – should therefore be based on the best existing business practices. For much of industry these would likely include:

(a) For basic voice communications – retention for at least six months, but no more than one year, as recommended in the EC draft, but only if the data types (discussed below) and other concerns are addressed

(b) For IP and email 'traffic' data[2] – no more than three months of IP address data, including e-mail traffic data (subject header, sender/recipient) originating on a provider's network if such could be supported by an impact assessment, to be supplemented by standardized processes and procedures for data preservation requests and access to preserved data

4) Any generalized obligation to retain data will be perceived by users as a significant impact on privacy, and hence have implications for their trust of electronic communications services.

(a) A mixed approach, combining current business practices for retention and a standardized preservation regime would generate a proportionate solution – comparable to several Member States and other global regions – and therefore mitigate potential impact on Europe's overall competitiveness.

(b) Further, standardized preservation that is limited to requests by law enforcement (with the appropriate legal substantiation), and access for criminal investigative purposes only, would respect Article 8 of the European Convention on Human Rights and Fundamental Freedoms.

5) The argument that mandatory data retention is not needed in the US, because there are no systemic data protection obligations requiring deletion of data, is a misrepresentation of reality.

[2] The Council text speaks to these types of data as 'Internet access' and 'Internet communications' data, respectively.

(a) Many large providers keep voice, IP and email data for the same type of business purposes on either side of the Atlantic, but do so at far shorter durations in the US than those proposed even in the EC draft – durations deemed acceptable by US law enforcement.

(b) Even after 9/11, and subsequent US legislative responses including the US Patriot Act, there is no mandatory data retention in the US. A system of data preservation is provided for in the legislation, which is supplemented by data retained according to industry business needs.

6) Similarly, the argument that data preservation would be inadequate as an investigative measure in the EU – given data protection-driven deletion requirements – is also untrue.

(a) Finland and Germany presently rely on data preservation-styled requirements without mandatory retention. Further, the Netherlands and German Parliaments and German and Austrian Constitutional Courts have severely restricted the ability of their countries to accede to European mandatory retention.

7) As the EC draft recognizes, retention of data must only be a part of any solution. Storage, security and retrieval requirements – and the physical location and manpower implications of each – must be taken into account when determining the investigative effectiveness and costs of retention.

(a) Cost reimbursement to providers must occur and apply both to capital and operating expenditures related to implementation.

(b) Industry looks forward to a detailed impact assessment to balance the investigative need for retention against its cost, and the EC has committed to such an assessment before adopting specific regulations.

(c) Service providers acting in conformance with a valid LEA request for access must be granted a waiver from liability to an end-user.

8) The EC draft recognizes that an ongoing dialogue among industry, LEAs and legislators will be critical to the success of any measure. This post-legislative dialogue or "dynamic legislative approach" will be necessary for three reasons:

(a) to gauge the need for continued retention, by analyzing the numbers of, duration for and investigative utility of retention requests;

(b) to affirm that reimbursement measures truly track actual costs; and

(c) to ensure 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.

The Quality of Industry co-operation with LEAs

Since the catastrophes of 9/11 and Madrid, and through recent terrorist atrocities in London, the communications industry has shaped a positive experience of co-

operation with law enforcement agencies (LEAs) toward the use of communications-related information to investigate criminal activity. As we raised in our comments of 15 September, to the EC's 30 July 2004 call for Consultation on mandatory data retention (Consultation Comments),[3] this co-operation has – in practice – nearly always been supported by existing industry business cases. These experiences were generated from our members and their discussions with European-based industry and other communications-related associations. For example, drawing from national law enforcement requests for access to and preservation of communications data, the following general statistics were presented in our comments:

- Roughly 98% of LEA requests for access to business-case retained data target only most recent few weeks prior to the request.
- Of the remaining 2% – requests target no earlier than 6 mos. prior to request.
- Only 2 cases arose in 5 years for access to business-case retained data older than 6 mos.
    - One of those requests was dropped by the LEA after the provider raised the costs that would be applicable to the search
- On average, the number of requests for retained basic voice data to a single provider is approximately 20 per week (e.g., France).
- On average, the number of requests for retained IP-related data is approximately 2 to 4 per month (e.g., France).[4]

Our comments regarding the applicability of business cases – particularly with regard to IP-related data – were reaffirmed most recently in comments from the American Chamber of Commerce to the EU (AmCham-EU)[5] and the 4 August "joint German industry comments" of BDI, BITKOM and VATM. As stated by AmCham-EU, the track record of service provider response to LEA requests suggests that, where companies keep data for billing purposes, this has proved to be both useful data and a sufficient time period. In practice, for IP-related data, this means a ceiling to any obligation of around 3 months for data that originates on a provider's network. Echoing this finding, the "joint German industry comments" cited (on the Council's initial draft requirement for retention of 1 to 3 years) that:

> The European Confederation of Police (EuroCOP) dismissed the draft of the Council, claming it would take too long to search the presently expected records and noting that there are numerous possibilities to circumvent the effectiveness of such a data retention regime. A study commissioned by the German Association for Information Technology, Telecommunications and New Media (BITKOM) likewise showed that LEAs hardly ask for data that are older than three months.[6]

Further, the efforts undertaken by communication service providers to support LEA preservation requests in the wake of the London attacks are unprecedented since

---

[3] A copy of these comments is located at: www.ustr.gov/assets/World_Regions/Europe _Mediterranean/ Transatlantic_Dialogue/Public_Comments/asset_upload_file557_7049.pdf.

[4] See note 3, page 14, of the Consultation Comments.

[5] A copy of these comments is located at: http://www.eucommittee.be/Pops/2005archive/dataretention 05302005.pdf.

[6] See these comments in full at: www.vatm.de.

9/11. Thus, the cooperative experience of industry and LEAs has affirmed that data retention according to present industry business practices is effective to advance the desired result: to provide effective means to combat terrorism.

The Need for More?

Some LEAs have made the argument that, in practice, law enforcement does not ask for access to data retained for longer than business cases because it knows it will not get it. This argument fails for two reasons.

First, the merit for law enforcement to make such requests would be to address one of the key existing legal hurdles to requiring mandatory retention, namely data protection. The Article 29 Working Party to the EC, the European Parliament, and the legal services of the EC and the Council have all affirmed that the Data Protection and Electronic Communications Data Protection Directives require "demonstrable need" in order for new legislation to derogate from the Directive's data purge requirements. These requirements stipulate that communications data, once it is no longer needed for the purpose for which it was collected, must be deleted within a reasonable period. For law enforcement to show a need for data older than that retained for business cases would serve to meet this burden in order to derogate from the need to purge. To-date, LEAs have not shown any demonstrable need for the length of retention described in either the Council draft or the six-month duration stipulated in the EC draft for IP-related data.

Second, in a very limited number of circumstances, law enforcement has indeed asked for more. However, of the very few LEA requests for data greater than that retained for business cases, law enforcement – in at least one case – has recognized the enormous attributable costs and withdrawn such a request. By contrast, several instances have been reported involving retention access and preservation requests from law enforcement that went un-used or ignored once the communications service provider compiled the necessary information at its own expense.[7]

A Harmonized and Proportionate Compromise

As detailed in ITAA's Consultation Comments, some Member State retention laws presently exist. The durations required under these retention regimes vary from one-quarter to one-half year (Netherlands, Switzerland); to 1 year (Belgium, Denmark, France, Spain, UK);[8] and two to four years (Ireland, Italy). In addition, all existing national laws in Europe differ widely as to *what data* is to be retained, often defining 'traffic data' – whether voice- or IP-related – very broadly. Indeed, despite that

[7] One such instance was raised by an anonymous ISP with regard to a voluntary request from the UK Crime Unit. After six months without pickup or response on the requested data, the ISP purged it given the immense hard disk space the retention required. See Digital Civil Rights in Europe, 14 July 2005, at: www.edri.org/edrigram/number3.14/preservation.

[8] Belgium's regulation on retention is as yet incomplete; France's one year requirement is both a minimum and a maximum and is awaiting finalization of its governmental decree; whereas Spain had tabled further legislation; and the UK program is voluntary.

multinational networks are transporting the data at issue under national mandatory retention rules, there are no harmonized requirements in Europe.

Thus, despite that ITAA continues to substantively object to the concept of mandatory retention obligations, a harmonized framework on both points (duration and definitions) is necessary. A legislative measure that harmonizes existing Member State laws, and blends the most acceptable components of the Council and EC drafts, should therefore be based on the best existing business practices. As we stated in our Consultation Comments, any duration should be a ceiling (not more than 3 to 6 mos.), not a suggested scope. This concept – of a European durational ceiling – is adopted in the EC draft. Further, the durations of six months and one year, for IP and voice-related data retention, respectively, come closest to those supported by industry business cases and the "demonstrable need" of law enforcement, as discussed above.

- Definitions

Irrespective of the retention durations proposed by both the Council and EC, any harmonized data definitions must reflect the current technical ability and business cases of communications service providers. Both the Council and EC texts have emphasized that only such data are to be retained that can be processed and stored without additional effort for the industry. In order to purportedly limit extra costs, the proposals would require companies to extend the retention period of data already processed and stored for other reasons. However, this approach is not truly reflected in the types of data addressed in both texts. For instance, as raised in the joint-German industry comments of 4 August (by BDI, BITKOM and VATM):[9]

All types of communications:

Storage of unsuccessful connection attempts – The storage of this data is presently prohibited under the data protection laws of several Member States because it is not necessary for billing purposes. Further, in order to make this data available, companies would have to fundamentally rebuild switching centers. The resulting costs to industry would be within the three-figure million Euro range exclusively for this type of data. In addition, LEAs have not shown a need for this information in light of these substantial costs.

Storage of the type of communication used (e.g., voice, fax etc.) – This information is recorded within the network only if it is relevant for billing purposes (e.g., as in the case of an SMS). In most cases (e.g., whether a connection was used for voice or fax transmission), the data are not available within the network. Making it available would require substantial technical upgrading.

Mobile communications:

Storage of cell ID during or at the end of a call – This data, as well, is currently not recorded or processed within most networks because it is not necessary for billing purposes. Recording this data would also require substantial technical upgrading. Further, LEAs have not shown an added value for this data set, as the retention of the cell ID at the beginning of every call already suffices to establish a movement profile. Further, there is no justification to oblige companies to supply

[9] See these comments in full at: www.vatm.de.

"data mapping" to a specified geographic description of the cell with each cell ID. Instead, it should suffice that LEAs are enabled to gather this information from a pre-submitted list.

Storage of the IMEI (communication device number) – The added value of IMEI retention, in addition to the telephone number, in order to identify a user is questionable at best. For this very reason, German LEAs in particular have departed from requesting IMEI data during expert discussions held in Germany.

Internet:

Storage of communication data of the Internet services used – Communications data of the Internet services used (i.e., who retrieved which website and when) is not retained on the network. Technical facilities to record, retain, and analyze this data would first have to be created and would subsequently lead to an astronomical rise in the volume of data to be stored. Indeed, it has been estimated that the burden of retention for this data set – also known as IP session data – for the UK alone would bring most networks to a halt within hours. Further, storage of websites retrieved would also reveal the content of a communication between the user and a network location. This conflicts with the assertion by the EU institutions that an interception of the content of communication should not be part of any data retention scheme.

Storage of MAC or any other device number – The device numbers of the network card of a computer (MAC) are, in contrast to an IP address, not even transmitted to most service providers. In order to change this reality, it would be necessary to reform both the Internet protocol and the existing infrastructure. Further, the added value of a MAC, in addition to an IP address as an identification-related investigative tool, has never been demonstrated.

- Durations

Recognizing that the applicable data type issues discussed above must be addressed in order to set durations that are proportionate (appropriate to both business cases, privacy requirements and LEA needs), ITAA provides the below.

For IP and email 'traffic' data, such a business case for retention would limit the duration to three months of IP address data (including at most three months – but likely less, depending on results of an impact assessment – of e-mail traffic data) originating on a provider's network.[10] This duration, briefer than that suggested in the EC draft, is necessary due to the inclusion of email traffic data (subject header, sender/recipient) within the scope of retained IP data. Because email 'traffic' is included within this definition, the EC's requirement for 6 months would represent a major departure from existing business practices. The systems are simply not in place to collect this sort of information, and the costs attributable to such a fast growing data set would be dramatic.[11]

Were the definition of IP data in the EC draft to not include email traffic, a retention period of six months for retention of IP identifier information would perhaps be sustainable. However, many providers do not presently retain even a week's worth of email traffic data originating on their network for business cases. For those

[10] The Council text speaks to these types of data as 'Internet access' and 'Internet communications' data, respectively.

[11] See the ITAA Consultation Comments, site listed at note 3, for a comprehensive discussion of the technical issues related to such data collection and how these issues impact costs.

providers that do have the technical ability to retain such data, the applicable storage and retrieval costs for the requirement will be significant. In suggesting that the duration for IP data retention – inclusive of email 'traffic' data – be lessened to three months, ITAA recognizes that the EC's draft could supplement by incorporating standardized processes and procedures for data preservation requests and access to preserved data.

For data related to basic voice communications, a business case applicable to both the Council and EC draft durations of six months is likely sustainable by many communications service providers in Europe, with one year perhaps sustainable by the largest providers. However, these statements recognize that the data type issues raised above would need to be addressed first.

Addressing Privacy Concerns by Standardizing Preservation

Any generalized obligation to retain data will be perceived by users as a significant impact on privacy, and hence have implications for their trust of electronic communications services. A mixed approach, combining current business practices for retention and a standardized preservation regime would generate a proportionate solution – comparable to several Member States and other global regions – and not therefore have an excessive impact on Europe's overall competitiveness.

Data "preservation" is the going-forward collection of data for a specific case and for a finite period, as supplemented by data retained according to business cases. Globally, data preservation is still the preferred method for investigative cooperation, and several Member States already prefer it over retention (e.g., Finland, Germany). Preservation was also advocated in the Council of Europe's Cyber-crime Treaty as a less intrusive and less costly alternative to data retention. In each of the national regimes that prefer preservation – including the US, Japan and Member States of the EU – access to data that may be retained (according to business case) or preserved is limited to law enforcement and for criminal investigative purposes only, under a clear process for an LEA to achieve the requisite authority. These principles of limited access under strict procedural controls were also reflected in the Council's most recent advocacy of a 'European evidence warrant', which would permit a judicial authority in one EU state to order that materials be handed over from another. Further, law enforcement can only require preservation to pursue a criminal case, and liability waivers are available for service providers who make data available on the basis of a valid LEA request.

Such process and procedural controls on access to preservation and limited retention act to curtail potential abuses and privacy concerns. Standardized preservation in the EU that is limited to requests by law enforcement (with the appropriate legal substantiation), and access for criminal investigative purposes only, would respect Article 8 of the European Convention on Human Rights and Fundamental Freedoms. In addition, mandatory retention – if implemented under harmonizing EU legislation – would further address related concerns if retention definitions and durations are brought closer to business cases and coupled with such standardized proven preservation schemes.

The argument that mandatory data retention is not needed in the US, because there are no systemic data protection obligations requiring deletion of data, is a misrepresentation of reality. Many large providers keep voice, IP address and some email data for the same type of business purposes on either side of the Atlantic, but

do so at far shorter durations in the US than those proposed even in the EC draft – durations deemed acceptable by US law enforcement. Even after 9/11, and subsequent US legislative responses including the US Patriot Act, there is no mandatory data retention in the US. A system of data preservation is provided for in the legislation, which is supplemented by business-case retention.

Similarly, the argument that data preservation would be inadequate as an investigative measure in the EU – given data protection-driven deletion requirements – is also untrue. Finland and Germany presently rely on data preservation-styled requirements without mandatory retention. For similar reasons concerning privacy-related impacts, the Netherlands and German Parliaments and German and Austrian Constitutional Courts have limited the ability of their countries to accede to European mandatory retention. On 27 July, the German Constitutional Court rendered a decision that several restricts the possibility of state law enforcement to use general surveillance measures – like retention – on telephones to prevent criminal activities. In contrast, both chambers of the Dutch Parliament have explicitly forbidden Dutch Justice Minister Donner from taking part in any Council agreement advancing mandatory retention.

Costs, Reimbursement and Ongoing Review

Industry looks forward to a detailed impact assessment to balance the investigative need for each type of data against the cost of retention. The EC has committed itself to accomplishing a thorough impact assessment before adopting specific regulations. This is the only reliable means to evaluate the consequences for industry and consumers and to analyze if and to what degree a European data retention regime helps to ensure effective police and judicial co-operation.

If the UK Government considers its present voluntary program for data retention in the UK satisfactory, as evidenced by a Home Office report on the program to Parliament, why do the proposed measures of the latest Council draft Framework Decision from the Presidency not reflect the program's definitions and principals?[12] The UK's voluntary code of practice has communications service providers retain details about, but not the content of, phone calls, emails and text messages. In turn, voluntary participants are not identified and cost reimbursement is addressed.

- Costs:

Extending the data protection-related security obligations of Directives 95/46 and 2002/58 to data retention – without cost and liability-related redress – would particularly force two critical issues:

a) Should companies be held liable for data they have not decided themselves to retain? *and*

[12] In comments made to the BBC on 11 July 2005, a Home Office spokeswoman stated that Home Secretary Charles Clarke's aim was "for the whole of the European Union to adopt similar measures" to the UK voluntary program (see "UK Urging Email Data Retention", at: news.bbc.co.uk/1/hi/uk_politics/4668903.stm). 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. This report has reportedly been issued but not made public to-date. The UK voluntary Code requires retention for up to 12 months (see Retention of Communications Data (Code of Practice) Order 2003 (SI 2003/N0.3175) (5 December 2003)).

b) If yes, should costs associated with different levels of security be included in the general cost assessment of proposed measures?

ITAA's Consultation Comments addressed the issue of costs – and their technological drivers – at length.[13] In addition, two studies have been undertaken this year to address this issue of potential costs due to mandatory retention proposals. One such study was conducted at the request of the Dutch government. The second is a reported cost study undertaken by the UK Home Office, the details of which have not been made public to-date.

The Dutch Ministry of Justice initiated its study, which was completed in late 2004 and released in April 2005.[14] The study report makes a clear distinction between costs for initial investment in retention-related technology and subsequent annual operational costs, which the costings do not address. However, the study does acknowledge prior industry estimates suggesting that operational costs could rise into the millions of euro annually for the largest national communications markets in Europe. As a baseline, the study evaluated ISP obligations that would flow from the Council's April 2004 draft Framework Decision, which included a one-year duration for retention of IP and email 'traffic' data. In addition, the study took into consideration three "security aspects" as cost imperatives: the confidentiality, integrity and continuity of the data to be retained.

The study estimated the total Dutch internet traffic at 25 Gb/s, and calculated that the initial investment alone for Internet providers to retain and store traffic data in the Netherlands would be at least 15 to 20 million euro. The study acknowledged that, as high as those costs might seem, they were already outdated when the report was finalized in November 2004 because they were based on KPMG analysis of statistics from 2003. The traffic at the Amsterdam Internet Exchange (AMSIX) has more than doubled in volume since 2003, mainly because of the success of broadband Internet deployment.

The AMSIX reported that they are now carrying about 70 Gb/s peering traffic over their infrastructure. At that rate, they estimate that the costs of retaining communication traffic data will keep rising sharply in the years to come, from maybe 40 million euro for all the Dutch ISPs today, to over a hundred million in a few years from now. Acknowledging the Dutch study and its estimate, the London Internet exchange, a powerful voice in the UK ISP community, suggested that the only way for ISPs to cover such costs without reimbursement would be to introduce a special user charge on customers.

- Reimbursement:

The EC text and Council draft's Article 16 are both welcome departures from past texts in that they begin to address cost reimbursement for industry for any retention mandates. Ensuring internal security is a core state function, which must be financed with public budget funds. Therefore, government must also bear the costs of data retention. Inadequate and non-uniform compensation within the European Union would otherwise distort competition, endanger long-term competition structures and prevent the furtherance of a uniform European internal market.

---

[13] See note 3, pages 9-13 of the Consultation Comments.

[14] The full text of the study report can be found at: http://www.bof.nl/docs/bewaarplicht_KPMG.pdf.

In advancing a phased-in approach to the most technically and economically difficult of retention requirements, the most recent Council draft also recognizes that an ongoing dialogue among industry, LEAs and legislators will be critical to the success of any measure. The EC text also includes a provision on a "platform" for discussion and review of technical abilities, the collection of statistics on implementation and costs, and a "review" clause for the legislation itself. This post-legislative dialogue or "dynamic legislative approach" will be necessary for three reasons:

(a) to gauge the need for continued retention, by analyzing the numbers of, duration for and investigative utility of retention requests;

(b) to affirm that reimbursement measures truly track actual costs; and

(c) to ensure 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.

However, under no circumstances would industry be best placed to provide statistics on the information required by LEAs. Tasks like this should be performed by the competent authorities themselves, or perhaps by a third party. For instance, only LEAs can demonstrate in which cases the information gathered from retention or preservation actually leads to successful investigation, an insight that is necessary to assess the effectiveness of any new investigative measure.

Conclusion

As evidenced in our Consultation Comments and above, the ITAA continues to believe that – given conservative privacy requirements and the economic and technical limitations of industry – data preservation is the preferred scheme for industry-LEA investigative co-operation. However, as we did in September 2004, the above comments on the current data retention drafts suggest way forward given existing myriad national retention obligations in Europe that are collectively unworkable for multinational industry. In advancing a way forward, given undesirable terrain unique only to Europe, the ITAA's comments complement nearly uniform positions taken at other international associations, including:

- ISPA-Belgium
- UK Communications Service Providers (UK-CSPs)
- Internet Service Providers Association of France (AFA)
- Euro-ISPA
- World Information Technology Services Alliance (WITSA)
- Competitive Telecom Carriers Association (CompTel)
- European Competitive Telecommunications Association (ECTA)
- European Communications Network Operators (ETNO)
- GSM Europe
- AmCham-EU
- Joint German industry comments of BDI, BITKOM and VATM

We commend these comments to your review as well, and look forward to renewed public dialogue at both the informal Council meeting in Newcastle on 8 September and any public forum the Commission should hold in September. Such industry meetings are needed as soon as possible, before a decision is made.

Thus, ITAA's comments are in no way an endorsement of mandatory retention as a concept. Many of the national members of ITAA's colleague organization WITSA

(the World Information Technology Services Alliance) would consider these comments far too liberal in that they accept the concept of retention as it exists in Europe. However, ITAA and WITSA members are not alone in advancing the view that mandatory retention has no place in an ordered society.

Recognizing and appreciating the plentiful objections to the concept of mandatory retention also continues to advance another question: If experiences with LEAs do not support greater retention, why demand it? This question was initially posed by the Article 29 Working Group in 2002. However, it has subsequently been repeated by the European Parliament, EC Directorates, and the legal services of the Parliament, Council and EC – LEAs have not still shown the necessary "demonstrable need" for retention.

Like our colleague international associations and others across the globe, the ITAA is horrified at recent events in London which echo the terror of 9/11 in the United States. In the ensuing days and weeks following 9/11, as industry, associations and the US Congress were considering legislation to advance new cooperative efforts between LEAs and industry to advance investigative measures, several key precepts from the 'founding fathers' of the US form of governance served to temper legislative fervor. Among these is a quote from Benjamin Franklin: "those who are willing to trade their liberty for a measure of security deserve neither liberty nor security." That simple statement, if taken as an absolute, would certainly be no more helpful than any other aphorism. But if taken as counsel of caution – as applied by others in recent past – it advocates continued deliberation on whether the impacts to privacy and vast technical and economic burdens are indeed warranted in advancing data retention, particularly as framed in the current draft texts.

Thank you again for the opportunity to provide these comments. If you have any questions please do not hesitate to contact ITAA's Senior Vice President for Global Affairs, Allen Miller, at amiller@itaa.org.