Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes

4 June 2003

Executive Summary

Issue
Many countries are issuing new obligations on communications service providers ("CSPs"– including Internet service providers) to store end-user traffic data for possible use by law enforcement agencies ("LEAs"). Mandatory retention, however, is neither economically efficient nor effective for criminal investigation. This coalition, therefore, urges governments to co-ordinate toward a data retention regime based on existing storage of end-user traffic data for legitimate business purposes and to seek advice and opinions from key industry stakeholders. Insufficient public input and multi-lateral harmonisation is likely to result in policies that harm CSPs and their end-users and impair a competitive and dynamic communications and IT services market.

Concerns
In addition to the lack of proper consultation with industry, there are fundamental concerns with many of the proposed traffic data storage regulations:
(1) scope of requirements (i.e., overly broad definitions of traffic data and excessive storage periods);
(2) (2) significant costs involved with storing and processing large volumes of data;
(3) Technical feasibility - how hardware and software modifications can accommodate data storage and processing requests; and
(4) Damage to end-user confidence due to privacy concerns and increased security risks involved with storing large volumes of data.

Recommendations
To address these concerns, any traffic data storage requirements introduced must balance the needs of LEAs, the capabilities and interests of CSPs, and the interests and rights of end-users. We support the following specific guidelines:

- Data preservation (i.e., targetted storage of specific data on specified end-users) should be favored over data retention (i.e., general storage of data for a specified period of time), because it is less burdensome and costly to business and less harmful to public confidence.

- Any requirement for data storage must be necessary, appropriate and proportionate, consistent with Articles 8 and 10 of the European Convention on Human Rights.

- Where countries have decided to institute laws mandating data retention, initial data retention periods and types of data to be stored should be limited to what is currently and routinely performed by industry for legitimate business purposes until adequate study and consultation with industry can determine whether longer retention periods would be necessary, appropriate and proportionate.

- Traffic data definitions (and storage periods) should be explicit and narrow, should exclude content and should relate directly to the mandating legislation.

- Governments should bear: (1) incremental infrastructure costs for mandatory data retention, (2) costs for data preservation from the point of preservation, and (3) marginal costs of requests to access stored data.

- Governments should maintain ongoing co-ordination with CSPs on technical capabilities to ensure that data storage and access requests are feasible.

- Governments should not impose data storage requirements on those communications services where obligations would impose unreasonably high costs or technological impediments, and would yield extremely low absolute and relative benefit. Examples of such services may include corporate/closed user group services and backbone services.

- Governments should seek internationally, and domestically harmonized traffic data storage rules in order to minimize CSP costs. Moreover, governments should limit traffic data requirements to deliverable outcomes without specifying how such outcomes are to be achieved (e.g., not mandating that traffic data be stored within a specific jurisdiction).

- Access to traffic data should be governed by lawful due process controls and limited to LEAs, on production of a warrant or similar instrument, and for the express purpose of investigating and prosecuting terrorism and other crimes.

- Governments should adequately train law enforcement officers requesting traffic data so that they are knowledgeable about the technological limitations of certain requests.

- Transparent and effective oversight procedures are necessary to prevent abuses and to safeguard public confidence.

I. Introduction

Over the past year, there has been a dramatic increase in the interest of countries, particularly in Europe, to impose obligations on Communications Service Providers (collectively hereafter, "CSPs") to store end-user traffic data for possible use by Law Enforcement Agencies ("LEAs"). Some countries have already issued new regulations to this effect, while others have stated intentions to adopt traffic data storage rules in the coming year.

Notwithstanding the on-going legislative and rulemaking activity across many jurisdictions, there is disappointingly little effort by governments to seek an adequately informed balance between the legitimate interests of government, CSP industry, and end-users. Business is concerned that the lack of co-ordination internationally and the low level of dialogue with experts from stakeholder groups will result in national policies on traffic data that severely harm CSPs, and in turn, their end-user customers. Business is committed to co-operating with law enforcement to combat crime and terrorism in a manner consistent with legal requirements, but is seeking to ensure that such legal requirements do not conflict with existing obligations to protect the privacy of customers or unduly harm a competitive and dynamic market for CSP services.

In addition to strongly encouraging a common international approach to data storage, and a closer dialogue between LEAs, CSPs, and end-users to match traffic data requirements with capabilities, business specifically identifies its concerns with the following aspects of potential traffic data storage regimes:
(1) scope of obligations;
(2) costs;
(3) technological requirements; and
(4) damage to end-user confidence.

This common industry statement argues that any traffic data storage requirements imposed by governments should be focused, well-defined, government funded, limited only to what is absolutely essential to protect society, and should balance the interests of LEAs, CSPs, and end-users.

II. Scope of Obligations

The scope of obligations is the most fundamental concern as it will ultimately define the costs, technological capabilities and end-user confidence. Within this category, there are three primary areas of interest:
(1) scope of relevant traffic data;
(2) scope of data storage period; and
(3) scope of relevant CSP services and data access.

Excessively Broad Definitions of Traffic Data:

Business is concerned that governments may define required "traffic data" very broadly so as to include any data related to a communication, and possibly content. Whereas CSPs may collect some sets of traffic data for billing or technical purposes, excessively broad definitions of traffic data will create uncertainty as to CSPs' obligations, lead to increased costs and technical burdens, and result in a non-transparent policy which may further damage public confidence in the privacy of electronic communications. Business therefore urges governments to narrowly define the traffic data types required to fight terrorism and crime, and to do so in a manner that reflects the traffic data that CSPs routinely capture and retain for business purposes. Data storage requirements should not exceed that which is necessary to achieve law enforcement objectives and which cannot be achieved by alternative and less intrusive measures.

Excessive Storage Periods – Data Preservation versus Data Retention:

The duration of the data storage period will determine costs and technological burdens on CSPs. Presently, jurisdictions are considering wide variations in their data storage proposals. Although some governments recognize that data preservation regimes[1] are entirely satisfactory for most occasions when LEAs require information from CSPs, a majority of governments appear to be favoring implementation of data retention regimes[2]. Of great concern is the variance and length of the proposed data retention periods, which range from 3 months to 3 years[3]. This lack of consistency in storage periods will be a significant additional burden on CSPs which operate in multiple jurisdictions. Further, these lengthy data retention periods strike the wrong balance between compliance burdens on CSPs and the associated benefits to LEAs.

Business urges governments to undertake, drawing on CSPs' expertise and experience, a meaningful cost benefit analysis of the impact of applying mandatory data retention requirements, and to conduct a similar cost benefit analysis to show whether alternative approaches, in particular that of "data preservation", could achieve the same objectives.

CSPs have a strong track record of fully complying with LEAs under national statutory arrangements. Compliance with legal requirements can include real time interception of communications and the preservation and disclosure of traffic data that is routinely collected for legitimate business purposes. This co-operation has proven effective.

---

[1] The G-8 has defined data preservation as when:
(a) upon lawful request by a competent authority,
(b) based on the facts of a specific case,
(c) specific historical data can be preserved to prevent its deletion,
(d) pending issuance of a lawful demand from a competent authority.
According to the G-8 definition, "preservation" does not include the prospective collection of data and does not obligate a service provider to generate data that it does not routinely require for lawful business practice.

[2] Data retention regimes, in contrast, require CSPs to keep and store all records of pre-identified types of data for an established and often lengthy amount of time.

[3] The Irish government has put in place a 3 year retention period by statutory instrument and is consulting on the introduction of primary legislation.

Where the retention of data is already mandated by law, countries should minimise the data retention period and the types of data to be stored to what is routinely performed for legitimate business purposes today[4]. Countries should also ensure that the conditions for storage, treatment, custody and provision of data to the competent authority upon lawful request are proportionate and do not result in substantial and disproportionate costs to CSPs.

Countries should favour data preservation over data retention - and in particular over any data retention that exceeds existing storage periods - because it is less burdensome and costly, less harmful to public confidence, it protects ordinary citizens, abides by national legal frameworks, is internationally consistent, and effective in satisfying LEA requirements.

Obligations for CSPs need to be proportionate:

As stated above, this coalition favours data preservation over data retention as a measure more generally proportionate to the relative interests of LEAs, CSPs and users. Mandatory data retention requirements that compromise the privacy rights of individuals and impose high costs or technological impediments on CSPs, or yield limited marginal benefits to LEAs would be particularly disproportionate, and should not be considered. Examples of services where such disproportionality may exist are as corporate/closed user group services and backbone services:

- In the case of communications services provided to entities such as corporations or B2B closed user groups[5], there are limited economies of scale from providing service to the group to defray high costs associated with data storage, and there is minimal likelihood that individuals would use the services of such groups to engage in or plan criminal or terrorist activity. Most closed user group customers have in place security and appropriate use measures. Given these facts, there is an unreasonably disproportionate burden and benefit to data retention.

- Likewise, backbone services have extremely limited visibility – if any visibility at all – to most categories of required data traffic. Moreover, to store the aggregate volumes of data they might receive would be technically infeasible, if not impossible. It is neither technologically nor financially practical to expect backbone providers to obtain, track or store data traffic relating to the end-users of their carrier/ISP customers.

[4] The new EU Directive on Data Privacy for Electronic Communications (Directive 2002/58/EC) clearly states that EU Member States wanting to impose mandatory data retention are restricted by existing Community law to strictly respect proportionality and human rights.

[5] Business to Business closed user group: group of corporations tied by a common business relationship such as, for instance, a car manufacturer with its upstream subcontractors and downstream car dealers.

Recommendations:

With respect to the scope of obligations governments impose on CSPs, business recommends the following principles:

- Data retention is an intrusive measure that should not be taken until less intrusive alternatives such as data preservation have been tested and proven insufficient to meet government's stated objectives.

- When a government requires data retention, it should be justified, limited, proportionate and necessary for the purposes of investigating and prosecuting terrorism and other crime only. The types and time periods of data to be retained should be kept to an absolute minimum, and not extend beyond what is necessary to attain the government objectives.

- The definitions of traffic data types to be stored or preserved, and the duration, should be well-defined, limited, and purposeful, and relate directly to the mandating legislation.

- Traffic data should be defined explicitly and narrowly to include only essential communication data fields and to exclude content data.

- Governments should not impose data storage requirements on those CSP services where obligations would result in unreasonably high costs or technological impediments or would yield marginal benefits to LEAs. Examples of such services would be corporate/closed user group services or backbone services.

- Access to traffic data should be restricted to LEAs, on production of a warrant or similar instrument under judicial authority, and for the express purpose of investigating and prosecuting terrorism and other crime.

III. Costs

Traffic data storage will result in massive costs. High costs to CSPs would harm competitive and dynamic markets, affecting end-user prices, driving some CSPs out of the market, and creating a barrier to entry for new and emerging CSPs.

In addition to significant traffic data storage costs, Governments should be aware that the most sizeable costs arise from searching and retrieving requested data from a significantly larger pool. Developing systems and processes for retrieving traffic data will involve substantial research and development, and also extensive hardware and software expenditure. The cost of introducing extra processing capabilities and training and administrative resources will also be significant. Operations with smaller economies of scale are unlikely to have the necessary expertise and dedicated resources to deal with requests for traffic data. If business were to bear the costs of services for law enforcement purposes, there may be insufficient economies of scale to allow some CSPs to profitably provide service in these jurisdictions. Further, for CSPs providing service in multiple countries, if countries fail to co-ordinate their respective national regimes, the worldwide compliance costs may make it unprofitable to offer entire categories of service on a global basis.

Mandatory retention of traffic data for periods longer than business requires not only magnifies costs, but also poses significant privacy and security risks by creating enormous pools of stored data, increasing the risk of illegal access to and misuse of this data. Governments and CSPs would need to develop appropriate security measures, at additional cost.

The extra costs and resources required may cause market distortion: deterring market entry by potential CSPs, causing smaller CSPs to fail, and creating substantial burdens for larger CSPs. Accordingly, governments must introduce appropriate mechanisms for CSPs to recover the costs arising from data storage for law enforcement purposes. Moreover, requiring LEAs to bear the cost of access requests to the traffic data will help to ensure that only strictly necessary requests for data are made, and will reduce public concern regarding the privacy implications of data storage. These safeguards will help ensure that goals of the use of stored data is limited to what is in the public interest.

Recommendations:

With respect to the costs imposed by traffic data storage requirements, business recommends the following principles.

- Where data retention regimes are in place, governments should bear the infrastructure costs of the mandatory data retention (and the ensuing maintenance costs), and the marginal costs of requests to access stored traffic data.

- Where data preservation regimes are in place, requesting agencies should bear the costs of data preservation from the point of preservation and not simply in the event of any subsequent request for the data.

- Governments should seek international co-operation on traffic data storage and access in order to minimise costs to CSPs and avoid market distortions. Likewise, governments should seek to minimise CSP costs by not mandating that traffic data be stored within their jurisdiction. Local data storage mandates in each jurisdiction would multiply compliance costs by several orders of magnitude.

- Governments will minimise costs with a framework of consistent requirement, a consistent information request format, and flexible rules as to where data may be stored. Governments should address requests to an agreed single point of contact in the CSP.

- Harmonised procedures for cross-border mutual assistance requests by LEAs will need to be developed, as this will reduce the likelihood of counter-productive, costly and technologically harmful requirements to redundantly store traffic data in multiple jurisdictions.

IV. Reasonable Technological Requirements

Governments should have a detailed and technical understanding that to store and to access vast amounts of traffic data will create significant technical difficulties for CSPs. These difficulties expand over time along with the amount of stored data. These difficulties increase for CSPs operating in multiple countries, if each country introduces its own national data storage requirements. CSPs also may have to deal with differing requirements between LEAs within the same country.

Unrealistic expectations by LEAs requesting traffic data need to be tempered by experience and by closer consultation with CSPs. Experience in several countries has shown that a lack of understanding of Internet network architecture, and of what data is useful, usable, or accessible to LEAs, can lead to unrealistic data storage measures and traffic data requests.

Accordingly, governments should work co-operatively with CSPs to develop workable solutions to the technical challenges of traffic data storage and retrieval requirements. Governments should better understand the cost and technical implications of their proposed measures, and they should better understand what data they can realistically expect to receive and use.

Recommendations:

To ensure that governments impose data storage requirements that are technologically and financially achievable, business recommends the following principles.

- Governments should co-ordinate closely with CSPs on technical capabilities. This co-ordination needs to be open and ongoing to ensure that data storage and access requests are feasible.

- All data storage requirements should include a process for determining whether an LEA request is reasonably achievable by a CSP for technical, financial or logistical reasons.

- Co-ordination between national data retention measures will reduce technological complications on CSPs.

- Governments should adequately train law enforcement officers requesting traffic data so that they are knowledgeable about the technological limitations of certain requests.

V. Damage to Public Confidence

There must be a relationship of trust between end-users and CSPs in order for communications networks to achieve their full potential to help society. Consumers and business users need to be confidant that their traffic data is confidential and secure, and that the likelihood of a security breach is minimal. Extensive types and time periods of traffic data storage can undermine this confidence in security. It is therefore essential to ensure that traffic data storage requirements are kept to the minimum levels essential to prevent terrorism and crime, and that the stored traffic data is available only to LEAs pursuant to a warrant or equivalent legal instrument.

Similarly, some large end-user customers manage their own IP addresses within the network provided to them by the CSP. When this is the case, LEAs may seek data traffic information held directly by the end-user (particularly if the information is not stored by the CSP), and CSPs will be inclined to protect the privacy of their end-users to the greatest extent permissible by law. If LEAs seek such information directly held by end-users, it is likely to generate significant security, privacy, procedural and cost concerns with the end-users storing the data. Before placing any requests for such end-user held data, LEAs should carefully consult with the CSPs and end-users to determine how best to minimise such concerns.

Recommendations:

To protect public confidence in the security and reliability of CSP networks, business recommends the following principles.

- Targeted data preservation regimes should be favoured over mandatory data retention.
- Transparent and effective oversight procedures are necessary to prevent abuses and safeguard user confidence.
- Access to traffic data should be limited to LEAs on production of a warrant or similar instrument, and for the express purpose of investigating and prosecuting terrorism and other criminal activity.
- Consultation among LEAs, CSPs and end-user customers is essential to balance interests of all parties.

VI. Conclusion

Business will assist LEAs in a professional and legally compliant manner. As LEA traffic data requests needs extend from the traditional fields of circuit switched voice traffic to the more complex and often less understood field of packet switched data traffic, it is essential that governments fully understand the cost and technological impact of requirements, and the proportionality of such requirements, before they decide to impose them. Thus, any traffic data storage requirements imposed by governments should be focused, narrow, government funded, limited to measures absolutely essential to protect society, and should balance the interests of LEAs, CSPs, and end-users. Business looks forward to all possible opportunities to work closely and constructively with governments to better understand and progress these important issues of mutual concern.

Background information on supporting organizations

ICC
International Chamber of Commerce
www.iccwbo.org
Founded in 1919, ICC is the world business organization, the only representative body that speaks with authority on behalf of enterprises from all sectors from over 130 countries around the world. Business leaders and experts drawn from the ICC membership establish the business stance on a broad range of issues affecting international trade. Dedicated to the expansion of cross-border trade, ICC champions liberalization of telecoms and development of infrastructures that support global online trade.

UNICE
Union of Industrial and Employers' Confederations of Europe
www.unice.org
UNICE is the official voice of more than 16 million small, medium and large companies active in Europe, employing over 106 million people. Active in European affairs since 1958, UNICE's members are 35 central industrial and employers' federations from 28 countries, working together to achieve growth and competitiveness in Europe.

EICTA
www.eicta.org
EICTA - European Information, Communications and Consumer Electronics Technology Industry Association - combines 44 major multinational companies as direct members and 29 national associations from 19 European countries. EICTA altogether represents more than 10.000 companies all over Europe with more than 1.5 million employees.

INTUG
International Telecommunication Users Group
www.intug.int
INTUG is an international association of users of communications technology and applications with an extremely wide constituency. Founded in 1974, its members include national users groups which represent the interests of users in Europe, the Americas, Asia-Pacific and Africa. Associate and individual members come from major multinational enterprises, academia, law and other relevant industry sectors. INTUG promotes the interests of all users at the international level and ensures that the voice of the user is clearly heard whenever communications policy issues are addressed.