International Chamber of Commerce
The world business organization

Policy Statement

Storage of traffic data for law enforcement purposes

Prepared by the Commission on E-Business, IT and Telecoms

Introduction

In the past 12 months many countries have been issuing new obligations for telecommunications and internet service providers, referred to in this document as communication service providers (CSPs), to store users' traffic data for possible use by law enforcement agencies (LEAs). A harmonized international approach which balances government, business and user interests is needed to ensure that storage of and access to traffic data for LEA purposes is adequate, effective and fair. Business is committed to co-operating with law enforcement to effectively combat crime in a manner consistent with business realities in a competitive, dynamic market and according to legal requirements. However, business is concerned that differing national policies on traffic data will create disadvantages for CSPs operating in countries with more far-reaching requirements and an impossible compliance burden for CSPs with operations in many different countries.

ICC's concerns regarding government requirements for the storage of traffic data are four-fold:

- Breadth of laws that could potentially be passed.
- Cost to business.
- Technical capabilities of CSPs.
- Damage to public confidence in electronic communications.

ICC urges governments considering data storage requirements to favour targeted data preservation over data retention regimes. Targeted data preservation is not only less costly and burdensome to business and less damaging to public confidence in communication networks, it also serves law enforcement's investigative objectives in a more straightforward and efficient way. Targeted data preservation is in accordance with the Council of Europe Convention on Cybercrime and is used in countries such as Canada, Australia, Singapore and the United States. Adoption by policy-makers of the points below will help to ensure effective co-operation on traffic data storage between government and business, and protect business and consumer confidence in electronic communications.

International Chamber of Commerce
38, Cours Albert 1er, 75008 – Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

What is traffic data?

Traffic data is the data created every time someone uses a communications system. It does not include the contents of a communication. Traffic data can include:

- the time, duration, and telephone numbers involved in a phone call;
- the email address of the sender and recipient of an email, and also whether an attachment was included;
- the location of a mobile phone, and, by inference, that of its user; and
- full or partial logs of web site addresses visited.

Broad definitions and wide-reaching laws

Business is concerned that governments may define required traffic data very broadly so as to include any data related to a communication. Whereas CSPs may collect some sets of traffic data for billing or technical purposes, open-ended definitions of traffic data will increase the cost and technical capability burden on CSPs, create uncertainty as to CSP's obligations, and further damage public confidence in the privacy of electronic communications.

Legislation introduced with the aim of giving increased powers to governments may be used to extend government powers beyond what is necessary to fight terrorism and crime. Business is also concerned that governments could introduce widespread requirements for data retention when law enforcement goals can be adequately met with narrower, more targeted powers of data preservation.

Recommendations:

- The definitions of traffic data to be stored or preserved, and also the time duration involved, must be specific, limited, and purposeful, and relate directly to the mandate of the enacting legislation.
- Storage of anonymous traffic data should not be required by governments because this data is not connected to identifiable persons and not of assistance with criminal investigations.

Data preservation versus data retention

Several countries are considering different proposals to create powers to require CSPs to store specific sub-sets of traffic data, for example, the communications of a particular individual or their communications after a certain date (data preservation), or to require CSPs to retain all the traffic data created by all their users (data retention). It is important to distinguish between these two very different data storage requirements. Data retention requirements mandate that CSPs must keep and store all records of certain types of data for a prescribed amount of time. Data preservation, on the other hand,

requests businesses to store or 'freeze' a subset of data pursuant to a specific government request. This preservation of a limited set of data is for a relatively brief period of time during which the government can obtain an order for disclosure of the data to law enforcement agencies.

CSPs co-operate already with law enforcement agencies by preserving and disclosing traffic data that is routinely collected for legitimate business purposes. This co-operation is very effective and there are very few occasions when CSPs are unable to satisfy a request to disclose traffic data because that data has been deleted. ICC members strongly believe that data preservation should be favoured because it is less burdensome and costly than data retention, and less harmful to public confidence.

Recommendations:

- Data preservation should be favoured over data retention as less burdensome and costly to business and less harmful to public confidence.
- Traffic data must be defined explicitly and narrowly to exclude, for example, content data, the data created when individuals make financial transactions using communications devices, and other types of related data such as decryption keys.
- Data retention must be justified, proportionate and necessary for the purposes of investigating and prosecuting terrorism and other criminal activity only. The types and time periods of data to be retained should be kept to an absolute minimum.
- Access to traffic data should be limited to law enforcement agencies on production of a warrant or similar instrument, and for the purposes of investigating and prosecuting terrorism and other criminal activity.
- Private CSPs, e.g. those serving closed corporate user group customers and not the general public, should not be required to retain traffic data. Traffic data retention requirements for private CSPs would impose unnecessary obligations on organizations such as universities and non-profit institutions which do not offer services to the public.

Cost to business

Traffic data storage is potentially a massive cost for business. Developing systems and processes for retrieving traffic data will involve significant research and development, and also hardware and software expenditure. The additional cost to business of putting in place extra processing, training and administration resources will also be significant, particularly for smaller CSPs. Mandatory retention of traffic data for longer than it is required for business purposes not only magnifies these 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. Appropriate security measures would also need to be developed, and at significant extra cost. The extra costs and resources required may cause smaller CSPs to fail, and create significant burdens for larger CSPs.

CSPs should not be required to bear the costs of data storage for law enforcement purposes. In the US and Australia, arrangements to reimburse CSPs for the costs of specific law enforcement investigations are already in place. Further, requiring the requesting law enforcement agencies 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 reduce public concern regarding the privacy implications of data storage.

Recommendations:

- Governments should bear the infrastructure costs of mandatory data retention regimes.
- LEAs should bear the marginal costs of access to 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.
- Particular attention needs to be paid to the cost burden on smaller CSPs. Smaller organizations will have little expertise and fewer resources, if any, to deal with requests for traffic data.
- Where required by law, CSPs retaining traffic data should be protected from civil and criminal liability of all types for these activities, for example, with respect to data protection legislation. Otherwise, this would impose conflicting obligations and create an impossible cost burden and level of risk for business.

Technical mandates and capabilities of CSPs

Storage of vast amounts of traffic data creates additional burdens and difficulties for CSPs. However, access to that data is the greater challenge. The technical difficulties and related costs of searching stored data increase exponentially over time and with the amount of stored data. CSPs operating in different countries are at risk of having to comply with multiple national data storage requirements.

Unrealistic expectations by law enforcement agencies requesting traffic data may need to be tempered. Experience in some countries has shown that a lack of understanding of Internet architecture and what data is useful and usable by law enforcement agencies can lead to unrealistic requests including, for example, the ability of a CSP to always link an IP address to a named individual.

Governments should work co-operatively with CSPs to develop workable solutions to the technical challenges of traffic data storage requirements. Governments should refrain from imposing 'one size fits all' technical solutions which impair the ability of business to meet traffic data storage requirements in a cost effective way and prevent consumers from obtaining the best possible products and services.

Recommendations:

- Where data retention is required, 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. Each jurisdiction should have a means to independently determine if data requests are beyond the technical or economic capabilities of CSPs.
- The types and time periods of data to be retained should be harmonized across all jurisdictions in line with current traffic data storage practices for legitimate business purposes.
- Harmonized procedures for cross-border mutual assistance requests will need to be developed, in consistency with the Council of Europe Convention on Cybercrime and other criminal justice mutual assistance agreements. For example, national central authorities for requests from abroad should be put in place in each jurisdiction to ensure that CSPs only deal with authentic and reasonable requests from the law enforcement body of the CSP's jurisdiction.
- Governments need to put in place adequate training for law enforcement officers requesting communications data, including for example the limitations of communications data storage, locations data for mobile phone users, deletion of log files and session information, and the ability to link I.P. addresses to identifiable individuals.

Damage to public confidence

Realizing the potential of communications networks depends on securing the relationship of trust between providers and users. Public concern about the privacy of communication and activities on the Internet has been widely expressed in the context of proposals for mandatory traffic data retention, and it is unlikely to diminish as more countries consider legislating on this issue. As business develops innovative new products and services which use the potential of modern communications networks, consumers and business users need to be confident that their traffic data is confidential and secure.

Recommendations:

- Targeted data preservation regimes should be favoured over mandatory date retention.
- Transparent and effective oversight procedures are necessary to prevent abuses and safeguard consumer confidence.

Conclusion

Any traffic data storage requirements imposed by governments should be focused, narrow, publicly funded, limited to the measures absolutely necessary to protect society, and balance the interests of government, business and users.

Document n° 373-22/106
18 November 2002