

In collaboration with



IP Data Retention for Compliance

Driving additional benefits for your business

Contents

1	Executive Summary	1
<hr/>		
2	Introducing IP data retention for compliance	2
<hr/>		
3	IP Data Retention	3
<hr/>		
4	Meeting the Challenges	5
<hr/>		
5	Going a Step Further	7

1. Executive Summary

Increasing complexity of electronic communications and an inconsistent approach to telecoms data retention across Europe has driven the European Union (EU) to release a new Directive. This aims to improve the investigation, detection and prosecution of serious crime through a harmonised set of requirements for the storage of data generated by telecoms and Internet service providers as a result of IP (Internet Protocol) communications on their networks.

Other countries are preparing laws for IP data storage. This will require a coordinated response by Government Departments and Law Enforcement Agencies to prepare for the new capabilities. Service providers will need to put in place facilities to capture the metadata generated by all IP communications including SMS, MMS, WAP, Web browsing, Instant Messaging and Voice-over IP. It must then be stored so that timely reports can be produced upon request by police and security forces.

The EU Directive requires nine states to comply by September 2007, and the remaining sixteen by March 2009.

The question of who pays for the investment by the service providers, and what the charging model might be, are just two of the issues that arise. And in fact if the capability to inspect and analyze each IP data packet in real-time is established for compliance, then a whole set of related business opportunities becomes available for a limited extra investment. These could generate additional revenues, reduce capital and operational expenditure, and improve customer satisfaction to the point that they encourage operators to develop a strategy for IP data retention and make the build investment early.

This white paper examines the requirements of the EU Directive, explores the issues raised, and invites those in Government, Law Enforcement and service provider organizations who will be affected by this to start planning.

2 Introducing IP Data Retention for Compliance

In many countries there is an existing requirement for telecommunications service providers to collect and retain details of traditional voice calls. This is an important tool in addressing serious crime.

Law Enforcement Agencies, responding to increased use of sophisticated communications by criminals, see the need to extend data storage to cover electronic data communications, which use a number of different IP standards.

In December 2005 the European Union (EU) adopted a Directive requiring member states to harmonise their data storage and to extend it to cover IP communications. Other countries are considering similar measures.

This white paper looks at the requirements of the EU Directive and considers the implications for regulators, Law Enforcement Agencies and service providers. It explores how business intelligence and reporting capabilities may be applied for law enforcement purposes, and considers other possible legitimate business opportunities for telcos and Internet service providers once the capability to capture, store and analyse IP communications data has been established.

3 IP Data Retention

Lawful obligations

Government regulators are extending the obligations on communications data storage to cover data generated as a result of all telephone, data and Internet communications. This will impact voice, data and Internet service providers.

The focus of this paper is on Data Retention, not to be confused with Lawful Intercept:

- Lawful Intercept means the possibility to intercept specific communication content when requested by legal authorities with a court order
- Data Retention is about keeping a record of the details of all communication details (not of the content of the communication) for a defined period of time

The need for a new European Union Directive

Advances in both electronic communication technology and sophisticated crime now require Law Enforcement Agencies to be able analyze detailed phone and Internet traffic in their fight against serious crime.

In the absence of a common approach to data retention in Europe, for example in terms of the type of data, storage period and conditions of retention, there was a need for harmonization through a common legal instrument to fight serious crime.

Directive 2006/24/EC of the European Parliament and of the Council of the European Union was drafted to address this, and was adopted by the European Parliament on December 14th 2005 under a fast-track procedure and endorsed by the EU Council of Ministers. It was published in the EU Official Journal on March 15th 2006.

What the Directive says

Providers of publicly available electronic communication services or of public communications networks must retain certain data generated or processed by them and make it available upon request to Law Enforcement Agencies—without ‘undue delay’—for the purposes of investigation, detection and prosecution of serious crimes. Certain aspects of the requirements are left to Member States to define in national laws.

This Directive makes data retention mandatory at EU level for both telecom and Internet service providers.

Data covered by the Directive includes all data generated, processed, stored or logged by a service provider when communication—including SMS, MMS, WAP, Web browsing, Instant Messaging and Voice-over IP calls—take place over publicly available networks for fixed and mobile Telephony, Internet telephony and Internet access. The data required is that necessary to identify the source, destination, date, time, duration, type of communication and location.

The Directive also covers unsuccessful call attempt data (for example calls that have been successfully connected but not answered or for which there has been a network management intervention). Unconnected calls do not fall under the scope of this Directive.

It is important to note that the Directive does not cover the content of the communications; this is prohibited. It is the metadata that is required.

The period of retention is between 6 and 24 months, and to be determined by national regulation. Storage for longer periods is possible if requested by member states and upon notification to the EU Commission. The data is to be destroyed at the end of the retention period.

The Directive declares that supervision rules are to be set up in each Member State. It is assumed that there will be a national authority to monitor retention schemes and audit IT retention systems in each jurisdiction.

Security and sanctions on providers

The Directive requires strong security features to protect retained data, for example against loss, disclosure, destruction, unlawful access and use. Access to data is the key element within this Directive as it is based on necessity and proportionality principles. Access must be given only to competent authorities (e.g. judge, police) and by authorized personnel only.

Dissuasive criminal penalties may apply for unlawful access, transfer of data, and unlawful further use or purpose.

Covering the costs of compliance

In principle, the Directive does not tackle the issue of reimbursement of the costs involved in compliance; this is left to the Member States. Full or partial reimbursement is however considered likely in most jurisdictions except Germany. Currently, negotiations have started locally between Ministries and individual operators. First indications appear to favor a 'fee per retrieval service' model, though details have yet to be developed.

Implementation timescale

The Directive sets two deadlines for implementation. The first, September 15th 2007, is applicable to both traditional telephony and IP data for all member states except the ones that have chosen to use the derogation for IP data. This derogation gives an extra 18 months to delay implementation of IP data. Hence, the second deadline, March 15th 2009, is applicable to IP data communications for member states that opted for this derogation at the signature of the Directive.

The member states that have chosen to implement both traditional telephony and IP data in one block for September 2007 are: Denmark, France, Hungary, Ireland, Italy, Malta, Portugal, Slovakia and Spain.

The member states that have chosen to delay IP data implementation until March 2009 are: Austria, Belgium, Cyprus, Czech Republic, Estonia, Finland, Germany, Greece, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Slovenia, Sweden, and the United Kingdom.

4 Meeting the Challenges

Establishing a set of IP data retention strategies and capabilities that are “joined up” and that meet the type of requirements specified, for example in the EU Directive, will present challenges at regional, national government, Law Enforcement Agency and service provider levels. Here we consider some of the issues raised.

Challenges for national governments

Governments will need to decide on their policy for data retention, and to define detailed regulatory requirements for the police, security services and service providers to work to. This is likely to involve consultation, for example to establish the meaning of “serious crime”, and decide how far to go in demanding and allowing data collection, storage and analysis.

For example the EU Directive calls for storage between 6 and 24 months. The latter implies larger data storage volumes and hence cost, but the Law Enforcement Authorities may press for longer rather than shorter storage periods. The regulator will need to balance the needs of the police and security services, service providers, consumers, businesses and other stakeholders, taking into account data protection and privacy sensitivities.

The issue of how much of the cost will be reimbursed and through what business model will be important, and regulators will want to consider to what extent to push for an aligned model across Law Enforcement Agencies as well as across service providers. Crime prevention across international borders will be of concern also.

Governments will need to clarify the rules for the major service providers with large networks and customer bases, and for small service providers such as WiFi hot-spot operators. And they will want to balance public pressure for crime prevention with that for data protection and privacy.

Other issues for Government include governance, inter-working between departments, measures to demand for supervision, audit of service provider retention systems, and penalties for non-compliance.

Challenges for Law Enforcement Agencies

Individual police and security service organizations will decide at local and national levels on their interpretation of the national requirements for data retention, and how they plan to use the data for effective investigation of serious crime. Decisions on harmonization of business models, and of tools for data management, analysis and reporting, may have a significant impact on the effectiveness with which organizations can co-operate nationally and internationally.

Law Enforcement Agencies will need to develop the skills, processes and tools to make and handle data requests. Specific technical challenges arise; for example how to deal with the use of encryption by sophisticated users.

Challenges for telecommunications and Internet service providers

For service providers, the Directive has various impacts that could be difficult to take into account, especially for small players. This involves cost and implementation aspects, in terms of infrastructure, people, processes and organization. Privacy and security measures will have to be implemented and are now mandatory for providers when retaining this data.

In developing a strategy for IP Communications Data Storage, a service provider will typically identify business and technical requirements, taking into account compliance needs, business opportunities, customer views and the business case. They will want to negotiate a business model for dealing with police and security services requests, including the basis for payments to ensure that their costs will be recovered.

Implementation by service providers

The technical capabilities required to usefully achieve IP communications data storage are broadly as follows:

- Network probes to capture the data from the network in real-time
- Data transfer to a data warehouse
- Data warehousing capacity to store the data
- Analytics and reporting tools to meet the internal and external business needs
- End-to-end process management to ensure compliance, performance and scalability

The tools to enable each of these capabilities are available and proven; the challenge will be to plan and implement seamless business and technical solutions in a pragmatic way.

Several practical issues are unclear to date and need to be defined nationally. For example, small service providers, such as hotels and Wi-Fi hot spot owners, may need to collaborate with larger network providers to deliver the required services. And many technical details need to be considered, for example should the subject of an email be considered as content or not? What data formats will be used? What are the arrangements for forecasting volumes, and planning for scalability, collection, aggregation and storage?

It is likely that service providers will try to negotiate with regulatory bodies in member states to minimize the impact of the Directive. However, too much divergence may disrupt the market.

5 Going a Step Further

Business and Technical Opportunities

Once the capability to capture, store and analyze IP communications data has been put in place, it can be a relatively small investment to extend this capability for legitimate business purposes to deliver deep insights into traffic and customer behaviour. This could result in significant business benefits, for example:

- Many service providers suffer from ever-increasing network capacity increase costs to cope with growing traffic volumes. Closer inspection of traffic patterns may reveal high volumes of low priority traffic, for example “spam” communications. Once identified these can be addressed appropriately.
- A better understanding of traffic and service usage patterns at a macro level may enable improved network efficiency and service design adjustments, resulting in reduced cost-to-serve, better customer service, and possibly new revenues.
- Detection of unusual traffic patterns may identify examples of fraud in real-time, enabling an immediate response.
- It may be possible to maximize return on investment for compliance by first creating a strategy to identify and collect data for business purposes (such as network utilization and fraud), prior to collecting data for compliance. This may, for example, justify keeping the data for longer than the period specified by regulation.
- It may be beneficial to build a single integrated data retention solution across multiple operating companies (such as mobile, fixed voice, broadband and Internet services), with minimal impact on operations and whilst ensuring compliance.
- It is possible to extend the capability to provide secure sensitive data for police liaison purposes.
- The ability to audit and collect all revenues associated with all traffic (circuit switched and IP) could prevent revenue leakage.
- Revenue growth through targeted marketing activities (subject to appropriate consent and compliance to data protection laws) may be desirable using newly available customer usage data on IP services.

There is also the possibility to deliver additional technical benefits, such as:

- The provision of cost effective and flexible long-term storage and retrieval—up to 2 years
- Advanced analytics, recognising that phone and Internet traffic analytics can be complex (for example VOIP and e-mail circles)

- The ability to provide fast access to intelligence for standard and ad-hoc reports and analysis to meet service level agreements with security agencies
- The provision of advanced system security, so that police liaison departments in a telco can have access to sensitive data, without making it available to anyone else (therefore minimizing leaks)
- The ability to provide information on IP service usage—potentially in real-time—to other business systems

Summary

The trend towards storage of IP communications data presents a significant opportunity for operators to drive revenue, retention, customer satisfaction and cost benefits through development of insights into customer behaviors and preferences. ISPs and Telcos with converged products are likely to have the greatest opportunities. They will be able to construct a 360° view of customer behavior that they could use for cross-selling, up-selling, advertising and communications with customers across a range of channels, subject to national laws and customer approvals.



About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of Consulting, Technology and Outsourcing services, has a unique way of working with its clients, called the Collaborative Business Experience.

Backed by over three decades of industry and service experience, the Collaborative Business Experience is designed to help our clients achieve better, faster, more sustainable results through seamless access to our network of world-leading technology partners and

collaboration-focused methods and tools. Through commitment to mutual success and the achievement of tangible value, we help businesses implement growth strategies, leverage technology, and thrive through the power of collaboration.

Capgemini employs approximately 61,000 people worldwide and reported 2005 global revenues of 6,954 million euros.

More information about our services, offices and research is available at www.capgemini.com.

Chris Jeffery

Global Head of CRM & BI solutions
Capgemini
Telecom, Media & Entertainment
chris.jeffery@capgemini.com
+44 (0)870 904 3626

Chris Parsons

CME Marketing Director, EMEA
Teradata
chris.parsons@teradata-ncr.com
+44 (0)207 725 8610