The EU data retention debate: Part one

Daniel Sullivan

Daniel Sullivan is admitted as a solicitor in Queensland and is currently undertaking LLM (Intellectual Property) studies at the University of Queensland.

"The EU data retention debate" will be published over two editions of *Computers & Law*, concluding in our September 2002 edition.

1 Introduction

According to the website www.statewatch.org, there is a real possibility that all phone calls, mobile phone calls, faxes, e-mails, web site content, and internet usage within, from and to Europe will soon be recorded, archived and made accessible to law enforcement agencies for at least seven years. This article analyses the continuing campaign by law enforcement agencies (**LEAs**) and governments of the European Union (**EU**) to lay the groundwork for general, wide-scale data retention. Part 1 of this article will consider:

- the nature of the data in question and its value to criminal investigations and intelligence operations by LEAs;
- the current regime of data protection in the EU and the proposed EU Directive on data retention; and
- the potential conflict between data retention, current European Commission (**EC**) data protection legislation and the fundamental rights of privacy and confidentiality of communications.

Part 2 of this article will be published in the September 2002 edition of *Computers & Law*. It will consider:

- the regime of data retention proposed by LEAs;
- the competing arguments for and against data retention; and
- possible solutions to, and the likely outcome of, the data retention debate.

This article will not examine the practical and financial implications of data retention.

2 Data retention

2.1 Overview of the debate

The pervasive influence of technology in our lives has raised concerns about the misuse of personal information that has been disclosed in the course of using that technology. The speed and ease with which data may be collected, categorised and shared presents a potential threat to citizens' privacy.

The right to privacy was not widely recognised until the adoption of international instruments such as the Universal Declaration of Human Rights (1948) and the European Convention on Human Rights (1950). The emergence of automatic data processing, facilitated by the development of computers, gave rise to agreements such as the OECD Privacy Guidelines (1980) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

The first EU data protection directive was implemented in 1995 (**the First Directive**), and applies generally to all individuals and organisations which process data. The First Directive requires that data relating to a particular individual should be deleted once the data are no longer needed for the purpose for which they were collected. This is called the "retention period obligation".

A subsequent data protection directive was implemented in 1997 (**the Second Directive**), which extended the retention period obligation to data associated with telecommunications. Under the Second Directive, data should not be retained by a communications service provider (**CSP**) at the request of a LEA unless it is required by law. The CSP is, however, allowed to retain the data for internal purposes such as billing, marketing and fraud prevention.

A proposal by the European Commission in July 2000 (**the Proposed Directive**) recommends that the Second Directive be updated to apply specifically to newer technologies such as the internet, e-mail, and satellite phones and that the retention period obligation be retained in the form of the Second Directive.

This Proposed Directive has caused alarm amongst both European LEAs and governments. The international law enforcement community is struggling to deal with computer crime in all its forms and considers that communications data should be retained for a substantial period of time to assist criminal investigations and intelligence collection.

Of particular concern to the LEAs is the fact that many internet service providers (**ISPs**) charge no fee or a flat fee for internet and e-mail services. This can result in communications data being deleted within a few hours of the end of a transmission, as they are not needed for billing purposes.

In 1995, the LEAs successfully imposed requirements on CSPs to have the technology to facilitate interception. LEAs are now waging a new campaign for long-term data retention. They have received support from some of the more powerful governments in the EU. The United Kingdom (**UK**) led the charge with a national plan to retain all communications data for seven years. This plan met with strong opposition from data protection bureaucrats, the communications industry, and "cyber-rights" advocates such as Statewatch and the Global Internet Liberty Campaign (**GILC**).

The data protection directives are discussed in detail in **3** below.

2.2 What is data retention?

A distinction must be made between data *retention* and data *preservation*.

Data retention requirements would oblige CSPs to collect and keep their data as a routine matter.

Data preservation involves keeping stored data protected from anything that would cause their current quality or condition to change or deteriorate. Data preservation requirements enable LEAs to instruct a CSP to preserve specified data already in its possession until the LEA secures the necessary authorisation (such as a warrant) to require disclosure of the data. To obtain the warrant, the LEA must have demonstrated to the warrant-issuing body that the specified data are likely to be relevant to a current investigation.

At present, CSPs do not have to retain data for law enforcement purposes and may delete data at will. This means that any useful data obtained through a warrant may be a matter of good luck. The later a warrant is obtained, the more likely it is that important evidence has been deleted.

Even the most vocal critics of data retention acknowledge that data preservation (preservation and interception go together) and interception on behalf of LEAs, subject to stringent safeguards, can be in the public interest. This article is predicated on the notion that current interception regimes, with judicial and/or parliamentary oversight, satisfactorily safeguard human rights and receive wide acceptance.

Data retention, on the other hand, constitutes both interception and data processing:

- the interception is very wide and may be seen as occurring at the time of retention, or retrospectively at the time that the LEA accessed the retained data; and
- the definition of "data processing" includes collection, recording, or storage of data.

On the one hand, opponents of data retention protest that it involves unacceptable generalised interception and data processing.

On the other hand, LEAs argue that data retention amounts to general data preservation and that no interception occurs until the safety barriers of the interception regime are overcome so as to allow LEAs access to the preserved data. Furthermore, LEAs contend that certain exceptions to data protection laws leave open the possibility of data retention.

2.3 What data is retained?

The main categories of data are:

(a) Content data

Content data are the actual contents of a communication, for example, the recording of a mobile phone call or the text of an e-mail message.

(b) Traffic data

Traffic data is that data spawned by the operation and administration of telephonic and computer communication services which is capable of being retained by the CSP, including the:

- type, starting time and duration of a communication, including time zone details;
- date of communication;
- data volume transmitted;
- subscriber data such as subscriber's number/identification, address and other identifying data;
- specific services used by the interception subject and the technical parameters for those types of communication;
- dynamic Internet Protocol ("IP") addresses;
- static IP addresses;
- geographical location of mobile subscribers;
- "Logical" location;
- number or identification of the other party to a communication for incoming and outgoing connections, even if there is no successful connection established;
- post-connection dialled signals emitted to activate features such as conference calling and call transfer;
- actual destination and intermediate directory numbers if communication has been diverted;
- call-diversion details including calls that traverse more than one network or are processed by more than one network operator before completing; and
- routing logs.

(c) Identification data

Identification data overlaps somewhat with traffic data. This category of information may currently be obtained by LEAs upon the production of a warrant. The focus of the data retention debate has been on technical traffic data. It is unclear how much of the following information would be required to be retained, but it is submitted that most of it falls within the "subscriber data" category above:

- names;
- postal addresses;
- phone numbers;
- e-mail addresses;
- credit card details;
- IP addresses;
- Personal Identification Numbers;
- passwords and user names;
- equipment data;
- port data; and
- account numbers.

Regardless of the technology of a communication, content data are susceptible to interception upon lawful authorisation.

Proposals for data retention, however, apply to traffic data only. It would be reasonable to assume that the retention of traffic data as opposed to content data would be more palatable to the average citizen.

Some partisan "cyber-rights" commentators have overstated their case by alleging or implying that content data will be subject to data retention. LEA proposals for data retention have not included content data. Even so, some of these commentators would still view the LEA proposals as the thin end of the wedge which would inevitably lead to retention of content data.

(d) Why is traffic data useful?

For crimes committed by computer, there is often no corroborative evidence other than traffic data. Traffic data may therefore provide the only clues as to the identity of the perpetrator.

Nearly all forms of traffic data may be altered or masked by a sophisticated criminal. Every piece of traffic data is

like a piece of a jigsaw puzzle. The more data there are to cross-check, the harder it is for a criminal to put police on the wrong track.

For example, a dynamic IP address may have been used by several different people, one of whom has committed a crime. To identify that person, the IP address and exact time of the transmission, at least, must be identified so that the CSP can match these details with the subscription details of the user at that time.

Use of retained data also extends to crimes not related to computer or communications networks, but where the data may help to solve the crime. The volume of data carried over the internet has been doubling in periods of less than a year. Many people today use personal computers for communication and storage of personal information. The traffic data from a victim's computer or telephone could help to build a personal profile of that person and yield valuable leads.

(e) Use of traffic data to solve crime

An EU Police Working Party document has described some of the ways in which traffic data can lead to the solution of a crime. Following are some examples in which suspects confessed to a crime upon being showed the incriminating technical evidence.

(1) Suspects can be "positioned"

A CSP was ordered to keep mobile phone location data and fixed network telephone data from several hours before and after a murder. This data confirmed that the suspects were near the scene when the crime was committed once those suspects were able to be identified several months later. Suspects can be positioned even if a mobile phone is in standby mode and no calls are being made.

(2) Suspects can be traced back from the victim

A girl advertised babysitting services on a Minitel (a popular interactive TV service in France) server. A man rang her home to arrange a time for babysitting. She was found raped and murdered. Police traced links to the Minitel server and obtained a court order obliging the phone operator to ascertain the identity of callers to the home that night. Erasing traffic data would have left only witnesses, rumours and anonymous calls.

(3) Identification of equipment used can implicate suspects

Anonymous or falsely registered prepaid mobile phone cards are widely used by criminals. Sometimes they constantly switch between several cards. Retained technical data could be used to identify the actual phone used thus linking the suspect with the incriminating calls.

(4) Cross-checking of data can disclose a suspect's identity

Correlation between police traffic data and a suspect's traffic data can be used to fix the identity of a suspect. For example, the French police sent a message over the Internet to a suspected Swedish paedophile who used pseudonyms. By noting the IP address and time of transmission of their message, the police, with the assistance of the CSP, determined who received the message.

(f) Traffic data as evidence

Traffic data may constitute at least four different types of evidence:

(1) primary evidence, for example, evidence of a crime committed by computer, locating a mobile phone user at the scene of a crime at a particular time;
(2) corroborative evidence, for example, proof of association of criminals by telephone contact;
(3) intelligence, for example, identifying and tracing associates and locating places of significance; or
(4) post-trial evidence, for example, to support appeals against conviction and investigations into miscarriages of justice.

3 Data protection in the EU

As noted above, practical privacy protection at the EU level is found in the two European Commission (**EC**) data protection Directives.

3.1 The First Directive

The First Directive harmonises protection of the right to privacy across the member states of the EU. It applies to all forms of data, regardless of the type of technology (if any) in which the data are embodied.

Every citizen is a "data subject" with regard to his or her personal data. "Personal data" are a form of content data and include any information relating to an identified or identifiable data subject. An identifiable data subject is one who can be identified by reference to an identification number, or to factors specific to the data subject's physiological, mental, economic, cultural, or social identity. Data subjects have the right to:

- access the personal data;
- know where the personal data originated; and
- have inaccurate personal data rectified.

Data may only be collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with the purpose(s) for which the data were collected (**the purpose obligation**).

Personal data must not be kept longer than is necessary for the purpose(s) for which the data were collected (**the retention period obligation**).

The First Directive is aimed at commercial activities, and does not apply to processing operations concerning national security, defence, and law enforcement. This is because measures undertaken for the purposes of national security, defence or law enforcement do not fall within the scope of the EC treaty, and the EC can only take action where a corresponding competence has been conferred on it.

There are no comparable data protection provisions for data processed for security or law enforcement purposes.

The scope of any obligation or right arising out of the First Directive (including the purpose obligation and retention period obligation) may be restricted by national legislation. It is a principle of EC law, however, that any exception allowed by the Directive will be interpreted restrictively so that LEA activities for purposes other than or exceeding security or law enforcement would be governed by the First Directive.

3.2 The Second Directive

The Second Directive complements the First Directive and extends data protection principles, rights, and obligations to the telecommunications sector, including the internet, but not including radio and television broadcasting.

It seeks to ensure that consumers will have confidence that telecommunications services such as video-on-demand, interactive television, digital mobile networks, and the internet will not present an unacceptable threat to their privacy.

An important right enshrined in the Second Directive is "confidentiality of communications". In particular, member states must prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, without the consent of users, except when legally authorised. The right to confidentiality of communications applies to both content and traffic data.

The retention period obligation requires that traffic data relating to subscribers and users stored by the CSP must be erased or made anonymous upon termination of the call, subject to certain exceptions.

Data may be retained for the purposes of assisting the CSP in determining subscriber billing and interconnection payments and resolving associated disputes. In addition, traffic data may be retained to assist the CSP to protect itself against fraud and to market its services with the consent of the subscriber.

In the case of the billing exception, the data may be processed up to the end of the period during which the bill may lawfully be challenged or payment may be pursued. The usual period is thirty days, although there is variation across the EU ranging from 14 days to 10 years. In most cases, there is no mandatory retention period imposed on CSPs.

For flat rate or free-of-charge access to telecommunications services, there is no need to retain data to determine payment amounts. Consequently, CSPs in this situation are, in principle, not allowed to retain traffic data unless they need it for another valid purpose.

Similarly to the First Directive, the Second Directive does not apply to national security, defence, and law enforcement. Legislation dealing with these matters can restrict rights (such as confidentiality of communications) and obligations (such as the obligation to erase or anonymise data) provided for by the Directive.

In summary, CSPs are not allowed to collect and store data for law enforcement purposes only, unless specifically required to do so by law.

3.3 The Proposed Directive

If implemented, the Proposed Directive would supersede the Second Directive. It is not intended to change the substance of the Second Directive but rather to adapt and update the existing provisions in a technology neutral way to new and foreseeable developments in publicly available electronic communications services and technologies.

Most importantly, the right to confidentiality of communications and CSPs' obligation to erase or anonymise data remain unchanged.

The term "establish a call" in the Second Directive would be changed to "transmission of a communication" to reflect technological plurality and so that "call" will not be interpreted restrictively to include circuit-switched connections only (eg. traditional voice telephony) and not packet-switched transmissions (e.g. the internet).

Under Article 15 of the Proposed Directive, member states are allowed to adopt legislative measures restricting the scope of rights and obligations for national security and crime prevention reasons.

The Proposed Directive does not expressly oppose greater law enforcement access to retained data.

4 The fundamental right to privacy

Critics of data retention argue that it would infringe upon fundamental individual rights such as privacy. The right to privacy has been developed in Europe through instruments of domestic and international law. To assess the desirability of data retention, it is necessary to examine the origin and scope of the right to privacy.

4.1 International instruments

On a global international level, the right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights (1948) and the almost identical Article 17 of the International Covenant on Civil and Political Rights (1966) (**ICCPR**).

Article 17 of the ICCPR prohibits "arbitrary or unlawful" interference of privacy, which implies that the right to privacy can be violated in situations provided for by law so long as due process is followed.

4.2 EU and the ECHR

Of more immediate relevance to the EU is Article 8 of the European Convention on Human Rights (**ECHR**) which provides that:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

At present, the ECHR is the only effective instrument for the comprehensive protection of privacy in the EU.

The principles of due process and lawfulness are comprehended in the above article by the expression "in accordance with the law".

Two further requirements are introduced by the ECHR: purpose and proportionality. Any violation of the right to privacy must be committed for a purpose specified in Article 8(2) of the ECHR. In addition, the intrusion upon the right to privacy must be "necessary in a democratic society". This intrusion must be necessary, no

more than adequate, and proportionate in the sense that the violation of a fundamental right must be balanced against the public interest so as to determine whether it is justified.

The protection of fundamental rights provided by the ECHR is particularly important since it has been ratified by all the EU member states, thereby creating a uniform level of protection in Europe.

A national legal provision in breach of an ECHR right can be reviewed by the European Court of Human Rights. In the event of a breach of a right, a judgment may be handed down against the member state concerned and it may be required to pay compensation. Member states have declared that they will comply with the judgments of the European Court of Human Rights.

Most EU member states enshrine the right to privacy in their constitutions. However, the UK's lack of a right to privacy at common law or by constitutional convention makes any EU legislative guarantee all the more crucial in that nation.

4.3 ECHR case law

It is possible to derive a number of general principles relating to privacy in the context of interception and data retention from decided ECHR cases and other sources:

(a) When does an interception violate privacy?

The definitions of "private life" and "correspondence" in Article 8(1) of the ECHR extend to telecommunications.

Any interception of communications, including the recording of data for the purpose of interception, represents a serious violation of an individual's privacy. The recording of traffic data, just as much as the recording of content data, is a violation of the right to privacy.

(b) When is interception justified?

Member states may only interfere in the right to privacy for the purposes listed in Article 8(2) of the ECHR.

Although national security can be invoked to justify an invasion of privacy, the principle of proportionality also applies. The national security interest must be weighed up against the seriousness of the invasion of individual privacy.

Invasions of privacy need not necessarily be restricted to the absolute minimum, but mere 'usefulness' or 'desirability' is not a sufficient justification.

(c) How far should interception go?

The least invasive means appropriate must be employed to achieve the objective.

Even if the interception of all telecommunications represents the best form of protection against organised crime and is permissible under national law, it would breach Article 8 of the ECHR.

Only in a "police state" is the unrestricted interception of communications permitted by government authorities, although the idea of a police state is repugnant to the overall objectives and principles of the EU.

(d) Legal basis

Interference in the exercise of the fundamental right to privacy may be permissible if there is a legal basis under national law specifying required circumstances and imposing appropriate conditions.

For there to be a legal basis for interception, there must be sufficient evidence that a crime has been committed by a specific person. A warrant or similar authorisation is required, which lays down precise details of limitation of the interception.

(e) Law and the citizen

The law must be generally accessible and its consequences must be foreseeable.

(f) Safeguards

Adequate guarantees must be laid down to prevent misuse of the power to interfere with the right to privacy.

A careful consideration of private and public interests is required for activities that demand secrecy, and provision must be made for more stringent monitoring arrangements in these circumstances.

Safeguards are 'adequate' if the power to order telecommunications surveillance is reserved for the highest administrative authorities, the surveillance can be implemented only on the basis of a warrant issued by a judge, and if an independent body scrutinises the performance of the surveillance measures.

4.4 Summary

In summary, the retention of data constitutes a potentially serious violation of privacy. In order to be lawful in the circumstances, an act of interception must satisfy the following requirements:

- legal basis (including specificity);
- proportionality;
- necessity;
- the least invasive method (ie. no more than adequate);
- the relevant law is accessible to citizens;
- the consequences of breaching the law are foreseeable; and
- safeguards exist against abuse of the interception power.

This article will continue in the September 2002 edition of *Computers & Law*.