The EU data retention debate: part two

Daniel Sullivan

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

1 Introduction

Part one of "The EU data retention debate" was published in the June 2002 edition of *Computers & Law*. Part one discussed:

(a) the nature of the data in question and its value to criminal investigations and intelligence operations by law enforcement agencies (**LEAs**);

(b) the current regime of data protection in the EU and the proposed EU directive on data protection; and

(c) the potential conflict between data retention, current European data protection legislation and the fundamental rights of privacy and confidentiality of communications.

This article continues below. It will examine:

(a) the regime of data retention proposed by LEAs;

(b) competing arguments for and against data retention;

(c) the recently implemented EU directive on data protection; and

(d) possible solutions to, and outcomes of, the data retention debate.

2 The campaign for data retention

In 1995, the Council of the European Union passed a resolution on the lawful interception of communications. It set out a number of "Requirements" which imposed obligations on telecommunications providers to configure their equipment and procedures in order to assist LEAs with the interception of content and traffic data.[1] The Requirements were developed by the FBI and have been part of United States law since October 1994.

Interception of data under the Requirements can only commence upon the production of an "interception order" which relates to the target service used by an "interception subject". The Requirements do not provide for the wholesale retention of data. The safeguards present in interception legislation are activated when the Requirements are used.

European Ministers in the Council did not meet to discuss the Requirements. Rather, they were agreed by an exchange of telexes in January 1995. The Requirements remained secret and were not officially published until November 1996. The European Parliament was not consulted at any time.

Since 1995, several attempts have been made by LEAs to update the Requirements. These attempts have struggled for political support because of the secretive way in which the Requirements were initially adopted. The push for data retention has grown out of attempts to update the Requirements and has also been conducted in a secretive, uncooperative manner by LEAs.

3 A proposal for data retention

Apart from generally opposing the deletion of data, some LEAs have produced detailed plans for a system of data retention. For example, a report was produced by the National Criminal Intelligence Service of the UK in August 2000 (**NCIS Report**).

The NCIS Report argued that there was a "sound business case for the substantial retention of communications data". It agreed with the UK Data Protection Commissioner that the retention of communications data needed to be put on a clear legal footing by statute. In addition, the NCIS Report observed that Article 8 of the European Convention on Human Rights (**ECHR**) requires transparency in the law in order to ensure that the public are aware of the impact of data retention on personal privacy.

The NCIS Report proposed the following:

(a) **Data retained.** A communications service provider (**CSP**) should retain all communications data (not including content data) originating or terminating in the UK, or routed through UK networks, including any such data that are stored offshore.

(b) **Initial retention.** Communications data generated by, or routed through, a CSP's network should be retained by the CSP for instant access for a minimum period of 12 months.

(c) **Long-term retention.** Once data is 12 months old, it should be archived for retention for a further six years, making a total retention period of seven years.

(d) **Method of retention.** CSPs would have the option to either store archive data in-house or transfer it to a 'trusted third party' (either a government run data warehouse or a private contractor) who would then take full responsibility for access, retrieval, formatting, forensic integrity and production of evidence in court.

The UK appears to have abandoned the seven year retention period proposed in the NCIS Report and is now pressing ahead with a "voluntary code" applicable to CSPs, although data would only be retained for twelve months. France and Belgium also have plans for retention periods of at least twelve months.

4 The case for data retention

LEAs have put forward the following arguments as to why data retention is a necessary exception to the rights of privacy and confidentiality.

4.1 Evidence

(a) Lack of corroborative evidence

There are usually no human witnesses and no physical evidence to connect a suspected criminal to a crime committed by computer. In these circumstances, tracing and interviewing the suspect can only be done through access to communications data. Indeed, the main objective of an internet search is to establish the identity of the suspect. Furthermore, a suspect can alter or erase data swiftly if they become aware of being investigated.

(b) The 'billing exception' is of limited use to LEAs

Internet billing is less and less correlated to distance and destination. Internet service providers (**ISPs**) tend to favour flat rate billing or no billing at all. Traffic data which is no longer needed for billing purposes must therefore be deleted by ISPs. LEAs consider that traffic data is critical to criminal investigations and that important evidence would be lost forever.

(c) Analogy with forensic science

The use of communications data is analogous to the use of DNA to identify and prosecute the perpetrator of a crime, since each relies on the re-evaluation of evidential material, the significance of which has only recently become apparent.

(d) Inutility of alternatives

In the absence of data retention, LEAs would be required to serve a production order on a CSP where it wishes to investigate suspected criminal activity. Such an order would indiscriminately corral all data regardless of its relevance and the order would need to apply to several CSPs. This system would be unworkable and would cause greater infringements on personal privacy than a system of limited data retention.

4.2 Justice

(a) Appeals by defendants

The NCIS Report argues that criminal defendants may need to access retained data to resolve possible miscarriages of justice. The importance of such data may not have been ascertainable at the time of the original hearing and the absence of data retention may prejudice the right to a fair trial guaranteed by Article 6 of the ECHR.

(b) Other legislation provides adequate safeguards

This argument implies that data retention is acceptable so long as access to the data is subject to the same safeguards as interception.

4.3 Intelligence and crime prevention

(a) Intelligence and evidence gathering capabilities

According to the NCIS Report, deletion of data will have a disastrous impact on LEAs' intelligence and evidence gathering capabilities. Research of historical data and analysis of links with other agents and locations is vital to both reactive investigations into serious crime and the development of proactive intelligence on organised criminal activity and matters affecting national security.

(b) Globalisation of crime

The ability of criminals to conduct illegal activities through many different jurisdictions at once has been fostered by the globalisation of business, telecommunications and travel. The NCIS Report argues that data retention is the counterbalance needed by law enforcement to enable a geographically based agency to cope with such crimes.

(c) Loss of time in international matters

Internet criminals frequently send communications through the systems of several different countries in order to mask their identity and reduce the possibility of detection. Even if mutual legal assistance agreements allowed sharing of information between all the affected countries, this process would be complicated and time consuming. Instantaneous data deletion would therefore hinder law enforcement.

(d) Containment of crime

Criminals and their organisations exploit weaknesses in law enforcement techniques. Early loss of data would encourage criminals to commit electronic crimes with a low probability of detection.

5 The case against data retention

5.1 Data protection officials

The EU Data Protection Working Party and other data protection officials have made the following arguments against data retention since 1999.

(a) Balance between law enforcement and fundamental rights

Data protection officials are conscious of the important role that traffic data can play in the context of the investigation of crimes perpetrated over the internet but remind national governments of the fundamental rights and freedoms of natural persons, including privacy, confidentiality, freedom of expression and the presumption of innocence.

(b) Clear legislative basis

Directives should provide clear and predictable conditions for CSPs as well as for LEAs. Legislation exists in most member states defining the precise conditions under which LEAs may lawfully have access to data stored by CSPs for their own civil purposes. Any change in these conditions must be clearly indicated by a legislative act.

(c) Consumer confidence

Consumers cannot have sufficient trust and confidence in products and services if it is not clear who has access to confidential communications and in what circumstances that access is allowed.

(d) Conditions required to be met for lawful data retention

Article 8(2) ECHR contemplates that the right to confidentiality of

correspondence may be over-ridden for the purpose of crime prevention if the interception:

- has a legal basis;
- is demonstrably necessary;
- is carried out for a valid purpose; and
- is proportionate in the circumstances.

Consequently, routine long-term preservation of data by ISPs for law enforcement purposes must be forbidden. It would be disproportionate general surveillance of communications and therefore incompatible with Article 8(2) ECHR and the EU data protection directives (discussed in part one of this article).

Public authorities should be granted access to traffic data on a case-by-case basis and never proactively. Furthermore, any data retention should be subject to rules governing the period of retention of the data and their automatic destruction if no further authority has been given for their retention.

(e) Exceptions to data protection

Any exception to data protection should not itself become the new rule. Exceptions should be interpreted restrictively.

(f) Data deletion

Data retention periods for billing should be rationalised across member states, preferably set at three months.

The status quo should be maintained - data should not be retained only for law enforcement purposes and should be deleted upon the expiration of the billing period.

5.2 Cyber-rights advocates

Private organisations such as the Global Internet Liberty Campaign, Cyber-Rights & Cyber-Liberties and Statewatch strongly oppose data retention.

Apart from echoing arguments used by data protection officials, some comments include:

(a) content data and traffic data should be more clearly delineated;

(b) access to retained data should only be given for "serious" crimes;

(c) a consistent standard of judicial review is needed across the EU;

(d) traffic data has been used in the past to identify dissidents and persecute minorities; and

(e) LEAs have attempted to subvert the democratic principles of accountability and transparency in their campaign for data retention.

5.3 The European Commission

On 26 January 2001, the European Commission issued a communiqué to the Council and the Parliament. It urged a coordinated approach to the problem of cybercrime based on wide-ranging consultation. The communiqué :

(a) suggested that any measure providing for the retention of data for law enforcement purposes would need to incorporate the same safeguards as conventional interception because retention of data effectively allows for the possibility of "retrospective interception";

(b) noted that the European Parliament is sensitive to privacy issues and has generally taken a stance in favour of strong protection of personal data. The Parliament did, however, express an opinion in 1999 favouring a general obligation for ISPs to preserve traffic data pertaining to child pornography content for a period of three months;

(c) discussed the desirability of consistent data retention requirements across the EU;

(d) did not make a firm recommendation in respect of data retention; and

(e) proposed an EU forum in which LEAs, CSPs, civil liberties organisations, consumer representatives, data protection authorities and other interested parties would be brought together with the aim of facilitating discussion on computer crime issues including data retention.

The sentiments of this communiqué were not welcomed by LEAs and were a major catalyst in the renewal of their campaign for longer term data retention.

6 Legislative developments

The proposed directive on data protection (discussed in part one of this article) came into force on 31 July 2002 as Directive 2002/58/EC (**New Directive**), after both the European Commission and the European Parliament yielded to the Council of the European Union's demands for data retention despite the strong warnings of data protection experts.

National governments must comply with the New Directive by 31 October 2003. The effect of the New Directive is also to supersede the second data protection directive from 31 October 2003.

Article 15.1 of the New Directive provides that:

> "Member States may adopt legislative measures to restrict the scope of...rights and obligations...when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of [the First Directive]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on the European Union."

This article effectively makes data retention unexceptional. Routine

retention of data may be permitted by legislation and those data may be retained for a "limited" period of time of unspecified duration. The New Directive itself does establish a data retention regime. Rather, it allows national governments to pass legislation in contravention of the retention period obligation so long as the purpose of the legislation is covered by Article 15.1.

The references to 'community law' and Articles 6(1) and (2) of the Treaty on the European Union have been labelled "window-dressing" by critics, given that every directive must already comply with these enactments by respecting fundamental rights.

7 11 September

The consequences of the terrorist attacks in the United States on 11 September 2001 undoubtedly influenced the course and outcome of the data retention debate. The US government subsequently urged the European Commission to revise "draft privacy directives that call for mandatory destruction [in order] to permit the retention of critical data for a reasonable period".[2] However, there is no data retention obligation imposed on CSPs under US law.

Prior to the September 11 attacks, it was generally believed that the European Parliament would reject the position on data retention taken by the Council. The Parliament is the only body directly elected by EU citizens and has traditionally supported strong privacy protection. Perhaps even more striking was the change in the European Commission's position. In its original proposal for an updated directive, it had supported the continuation of the retention period obligation.

The perceived heightened threat of terrorism has led to new laws in many nations that restrict liberties in the name of national security. Security measures that would previously have been vigorously resisted are now likely to be readily accepted by political actors. It is reasonable to speculate that this new political climate has radically changed the outcome of the data retention debate.

8 Balancing human rights and data retention

The campaign by European LEAs for data retention has caused a great deal of concern amongst people who value privacy and confidentiality. It has been suggested that the wholesale retention of traffic data will slowly lead to a "police state" of an Orwellian character.

Human rights including privacy, confidentiality and data protection are firmly entrenched in European law. Any suggested imposition on those rights is rightly treated with great caution.

The real issue is: can governments be trusted? Even the most passionate opponents of data retention admit that LEAs have a responsibility to investigate and prevent crime and that carefully regulated violations of privacy and confidentiality may be necessary in order to fulfil that responsibility. If it could be guaranteed that retained data would not be accessed except for particular purposes in specified instances provided for by law, the dangers of data retention would be greatly reduced.

Unfortunately, some governments in democratic countries have historically been guilty of misusing law enforcement resources for political purposes. Like-minded governments could emerge in any European nation under the right circumstances.

The attitude of some data retention opponents has been that any assent to encroachments on human rights will signal the first step in a slow erosion of those rights. This will lead, it is said, to loss of confidence by consumers and businesses in e-commerce.

It should be noted that data retention relates to traffic data and not to content data. Some civil liberties groups have opted for sensation by implying that the content of every phone call, fax and e-mail will be kept for seven years. Content data can be intercepted under conventional interception procedures but will not be routinely retained for law enforcement purposes. Nevertheless, an analysis of traffic data can tell a lot about an individual, including their location, movements, equipment and association with others.

Technological data that can be used to spy on innocent people can also be a very effective tool in bringing criminals to justice. It is an extremely valuable tool for both reactive and proactive law enforcement strategies.

The solution to data retention lies somewhere between prohibition and unrestricted LEA access.

LEAs may well ask: why should valuable traffic data be destroyed if access to it is adequately regulated? Opponents of data retention ask: why should traffic data be retained once it is no longer needed for proper purposes?

The management of residual traffic data obviously needs to be put on a clear legal footing. Some CSPs delete data immediately for budgetary reasons while others have reached informal arrangements with police to retain data for a long period. This means that there are differences in data retention periods across the EU and within EU member states. Not only is this troublesome for law enforcement efforts, but it creates other dangers for society. Without clear regulation, a CSP might succumb to pressure or inducement from a LEA to provide inappropriate data, thereby constituting an uncertain threat to human rights. A uniform standard for data retention across the EU will provide better protection of such rights.

How should that uniform standard be guaranteed? Most data retention opponents have protested that data retention for law enforcement purposes infringes on data protection principles. However, it is a fact that national security and law enforcement fall outside the scope of the Treaty on the European Union. The data protection directives derive from the Treaty and cannot apply outside its bounds. There are no data protection provisions for law enforcement and national security. The European Parliament has pointed out on numerous occasions that this is an unsatisfactory situation.

The focus of data retention opponents, therefore, should not just be on the spirit of data protection but on the scope of the law enforcement

exception contained in the New Directive. The wide-scale data retention permitted by the New Directive is a viable alternative as long as it is strictly regulated.

9 Conclusions

As already noted, the European Parliament once commended a proposal for a three month retention period of internet child pornography data for police purposes although this retention would only take place once the CSP had identified the content as illegal. Similarly, a standard three-month retention period of traffic data for billing purposes has received support from European data protection officials.

It is submitted that a retention period of no more than twelve months is a reasonable compromise. A seven-year retention period would be considered unacceptable by most Europeans. If an errant government were in possession of only twelve months worth of traffic data at any one time, its capacity to retrospectively profile an opponent would be reduced.

In any case, access to retained traffic data ought to be strictly regulated. If the interchange of information between LEAs and CSPs is too free, LEAs and governments could start to look on CSPs as partners in a police state.

The barriers to access need to be comparable to the barriers that must be overcome to have an interception authorised so as to maintain the principle of the presumption of innocence. Authorisation should be given by a judicial officer. Additionally, there should be a data retention commissioner at both national and EU levels who are responsible for monitoring abuses of data retention. This commissioner should be given powers and independence such that a CSP is not afraid to report abuses by LEAs. Article 15.3 of the New Directive assigns this role to the existing EU Data Protection Working Party.

Opponents of data retention argue that retention of all traffic data for any length of time is disproportionate and is prohibited by the ECHR and principles of community law. If this is true, there is an inherent contradiction in Article 15, given that blanket data retention cannot possibly accord with the provisions cited in the Article. This could present a difficult situation for the European Court of Human Rights which may have to decide either that data retention is prohibited by community law, or that community law is overridden by the express words of the New Directive.

One way to resolve this conceptual dilemma is to concentrate on LEA access rather than the data retention itself. If data is retained for a limited period but is never examined by an LEA, could a data subject's rights be compromised? Technically speaking, the answer is yes, as retention falls within the definition of data processing. Practically speaking, however, LEAs stand little chance of intercepting a complete trail of criminal communications data when they are indistinguishable, perhaps deliberately so, from the communications data of law-abiding citizens.

It is suggested therefore that the best solution available is to allow data retention for a limited period of time (such as twelve months) with appropriate safeguards at the LEA access stage.

The conditions laid down in Article 15.1 of the New Directive (such as necessity and proportionality) are consistent with this solution. The question of whether such conditions have been met should be determined by a judicial officer at the time when an LEA requests access to stored data.

With these safeguards in place, the only issue left unanswered by the wording of Article 15.1 is the length of time that data can be retained. Data retention inevitably impinges on fundamental human rights such as privacy and confidentiality of communications. In the light of current security concerns, these rights have been, and will continue to be, restricted to some extent.

It remains to be seen whether the future standard period of data retention, whatever that may be, will achieve a satisfactory balance between privacy and security. It should be hoped that EU governments will have something tangible to show in the fight against crime in return for the restrictions they have succeeded in placing on their citizens' fundamental rights.

Postscript

On 19 August 2002, Statewatch (www.statewatch.org) placed leaked documents on its website relating to a proposed "framework" directive. It appears that the European Council is now lobbying for a compulsory data retention period (for traffic data only) of 12-24 months for all EU member states. Presently, under Article 15.1 of the New Directive, individual nation states are permitted, but not compelled, to make use of the data retention exception. It will be very difficult for any member or institution to resist the Council on this issue. It would seem that this proposal was deliberately kept under wraps and has been revealed only now so that it did not jeopardise the preceding campaign for a suitable law enforcement exception to data deletion.

---

1 See part one of this article for definitions of content data, traffic data and identification data.

2 *Text of US letter from Bush with demands for EU for cooperation* <http://www.statewatch.org/news/2001/nov/06uslet.htm> (7/3/2002)