COUNCIL OF THE EUROPEAN UNION

Brussels, 20 December 2004

8958/04
ADD 1

CRIMORG 36
TELECOM 82

ADDENDUM TO COVER NOTE

from :	the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom
date of receipt :	28 April 2004
to :	Javier Solana, Secretary-General/High Representative
Subject :	Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism

Delegations will find attached the explanatory note on the above initiative.

EXPLANATORY MEMORANDUM
FRAMEWORK DECISION ON THE RETENTION OF COMMUNICATIONS DATA
(doc. 8958/04)

1. INTRODUCTION

Data Retention

Data retention refers to the storing of communications data generated by communications service providers in the provision of their general services. The length of time that communications data are retained by individual communications service provider will vary according to a number of factors including business needs, platform capability and capacity and national legislation. Currently, across the European Union there is a large variance as to the length of time communications data is retained by communication service providers, both between Member States and within Member States.

Background

The European Union, made up of urban societies, with vulnerable infrastructures and permeable borders, is increasingly at risk from cross-border criminal activity. The need for a European-wide data retention policy was initially identified in response to this increase in the levels of international crime.

Coincidentally however, this Framework Decision has been developed at a time when the threat from terrorism has been in sharp focus. The Madrid bombings on 11 March 2004 served as a graphic illustration to Europe of the grave threat Member States now face from radical terrorist groups. This rising level of threat of terrorist attack reinforces, fuels and creates a sense of urgency with respect to the need for a European-wide data retention policy, rather than provides the principle basis for it. Consequently this Framework Decision is directed against both criminal activity generally and acts of terrorism.

It is clear that sophisticated international criminal and terrorist organisations, aware of the variations in legislative requirements between different Member States with regard to data retention regulations, will inevitably gravitate to Member States which allow communication service providers to operate networks with shorter data retention periods. Clearly this would be done in order to take advantage of the anonymity this will afford and so frustrate the efforts of any investigators attempting to follow their communication "footprints" either in order to place them at the scene of the crime or identify all associates and co-conspirators. Approximation of retention rules will both diminish the risk of the creation of these "data havens" within the Europe Union and perhaps more importantly ensure that evidence in the form of communications data will be available to facilitate judicial co-operation between law enforcement authorities.

As the threat from international criminals and terrorists has been increasing, coincidentally there have been significant technological changes within the telecommunications industry, a fiercely competitive sector. These developments have put pressure on service providers to reduce the time period for which they store their communications data. One example of the new technologies which is already impacting on data retention periods is the development of ‘pay as you go’ technologies. This is one of the major drivers for a reduction in the time that communications data is retained by the Industry; plus this payment option may in any case reduce the amount of data initially available.

These technology-based developments are in addition to the ever-increasing commercial demands that force businesses to continually assess and re-assess the value and efficiency of their systems. These commercial pressures to drive down costs also mean that communications data previously kept for business purposes is now being destroyed because its commercial value has diminished. However it is clear, that although these pressures exist and are mounting, they have not reached 'critical mass' in many companies and so although retention periods have been falling there has been no movement as yet towards slashing retention times. This Framework Decision will forestall such an eventuality. Preliminary research also suggests that although communications service providers may well have to increase their retention periods for some data types it is unlikely that compliance with this Framework Decision will require an extension of retention periods for all data types in all companies.

It is therefore crucial to enable Member States to deliver an area of freedom, security and justice and to succeed in their fight against crime including terrorism that legislation be introduced compelling all Member States to develop binding data retention provisions. With this aim in mind, recognising the international nature of communications service providers business, this Framework Decision will achieve approximation of Member State rules to ensure that this essential investigative tool is available in the event of a crime or act of terrorism being committed.

The objective of this Framework Decision

Communication service providers generate communications data through the everyday provision of their services. This data is currently stored for a number of reasons including the detection of fraud, the preparation of invoices and compliance with financial regulations. This Framework Decision contains measures that will require communication service providers to either maintain or extend the period of retention for certain of these communication data types.

Support for the introduction of binding rules on the retention of communications data has been growing and gathering momentum over the last few years. The argument has now been won and the importance of communications data as an investigative tool is now almost universally recognised and has been acknowledged in a number of forums. Perhaps some of the most important and most recent include the following.

On 20 September 2001 the Council adopted conclusions (document SN 3926/6/01) which recognised the importance of communications data in the fight against crime and terrorism. In addition it requested the Commission to submit proposals ensuring that law enforcement authorities are able to investigate criminal acts involving the use of electronic communications systems.

The importance of communications data was further acknowledged in Article 15 of Directive 2002/58/EC on privacy and electronic communications. Article 15 allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of the Directive, 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 Directive 95/46/EC.

During its meeting of 19 December 2002, the Council adopted conclusions on information technology and the investigation and prosecution of organised crime (document 15691/02). These conclusions identified that the maintaining and developing of the Union as an area of freedom, security and justice as laid down in Article 2 of the Treaty on European Union and the creation of the high level of safety in this area which is the general objective of Article 29 of the Treaty depends on the possibility to carry out criminal investigations and prosecutions sufficiently, thoroughly and effectively, while respecting human rights and fundamental freedoms as laid down in Article 6 of the Treaty on European Union.

These conclusions also noted with concern that the technological innovations brought about by the continuous development of the internet and other electronic communications services as well as the increase in electronic banking, in parallel with their great benefits to society, also make it possible for criminals, in particular criminal organisations to further exploit these technologies.

Furthermore the conclusions urged all parties concerned (governments, parliaments, law enforcement and judicial authorities, industry, data protection authorities and other interested parties), as a matter of priority, to engage in an open and constructive dialogue at national and EU level aimed at finding solutions to the issue of traffic data retention that satisfies both the need for effective tools for prevention, detection, investigation and prosecution of criminal offences and the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy, data protection and secrecy of correspondence.

On 25 March 2004 the European Council published a Declaration on Combating Terrorism in which reference was made to the importance of establishing rules on the retention of communications traffic data by service providers. It further stated that priority should be given to the development of this proposal so that adoption could be achieved by June 2005.

Legal Basis of the Framework Decision

The legal basis of the Framework Decision is the Treaty of European Union and in particular Article 31(1)(c) and Article 34(2)(b).

Data preservation is not a substitute for data retention

The view of the European Data Protection Commissioners published as Opinion 5/2002 argues in favour of data preservation rather than data retention. Data preservation is the storing of data relating to specified individuals rather than the 'blanket' storing of data required under a data retention regime. Data preservation as suggested by the Data Protection Commissioners is recognised by the security, intelligence and law enforcement agencies a very useful tool for investigating the activities of someone already under suspicion. However, it will never aid in the investigation of a person who is not already suspected of involvement with a criminal or terrorist organisation.

Data preservation is therefore not sufficient to meet the needs of the security, intelligence and law enforcement agencies in the fight against modern criminals including terrorists.

Furthermore, the existence of a data retention regime prevents the disproportionate use of data preservation. Here is a key element of data retention which is frequently misunderstood: in the data retention regime, the principle is that retained data are not, in principle, accessed by anybody. It is only for a very limited part of these data, and on a case by case basis, that law enforcement authorities may decide to look into this information. Without this regime, and taking into account the threats posed by new forms of criminality, including terrorism, there would be a growing need for an extension of data preservation where all information transmitted from or to a specific person is not only retained but also available for consultation by the authority which ordered the preservation.

2. ARTICLE 1 – SCOPE AND AIM

The objective of the Framework Decision is to ensure that data generated in the course of making or receiving a communication is retained by the communication service providers for a set period of time. This is to enable both the subsequent investigation of the communications data and facilitate judicial co-operation, should there be a legitimate need to do so for the purposes of preventing, detecting, investigating and prosecuting crime and criminal offences including acts of terrorism.

This article, in addition to identifying what is intended to fall within the scope of this Framework Decision, also identifies what does not fall within the scope of this Framework Decision. This Framework Decision does not deal with the interception of content of communications. In other words, this Framework is not intended to cover what is actually said or written in a communication.

The purposes for which communications data may be retained under the Framework Decision are set out in Article 15 of the Directive 2002/58/EC. As suggested above these purposes include preventing, detecting, investigating and prosecuting crime and criminal offences.

The purpose of 'preventing crime and criminal offences' is perhaps the only purpose that is not self-explanatory and may cause some confusion. Prevention of crime in the Framework Decision refers only to situations where there are reasonable grounds to suspect that a crime is being planned. In other words, suspects must have raised reasonable fears that a crime will be committed which then causes the suspects to be investigated by law enforcement agencies with the aim of foiling the plans. The concept of 'crime prevention' in the Framework Decision is not limited in terms of the types of crime falling within the scope of the Framework Decision.

However, it is also acknowledged within the Framework Decision that different legal positions exist across the European Union with regard to 'crime prevention' as a purpose of data retention. The Framework Decision attempts to accommodate these differences by recognising that it may not be appropriate for some Member States to adopt the principle of data retention for the purpose of 'crime prevention', inter alia because 'crime prevention' does not constitute a competence of the authorities which are dealing with special investigative measures which include the acquisition of communications data. A derogation has therefore been included in the Framework Decision allowing Members States the option of excluding 'crime prevention' as a purpose of data retention from their national law.

3. ARTICLE 2 – DEFINITIONS OF DATA

The data that is currently stored by the Communications Industry covers a wider range of data that they initially need to manage the operation of their networks and to enable a bill to be prepared. This information has been described in Article 2 of the Framework Decision and identifies the "who made what call, when, where and how" on each network or service. Each company may have tailor made retention needs for different data and the requirements for investigations into criminal and terrorist activities identify that the following data be retained for the purposes outlined in Article 1. That is, for the purpose of the Framework Decision data includes the following types of data; telephone numbers, internet addresses, billing addresses of the customer and the telephone numbers/communications called or made using that phone/computer.

In addition data which identifies the time a call/communication was placed, the length of a call/communication and the location of the sender and recipient phone is also included in the Framework Decision.

4. ARTICLE 3 – RETENTION OF DATA

This article identifies the need for these measures to be adopted by all Member states to facilitate the international judicial co-operation necessary in dealing with crime and criminal offences including terrorism, where criminal conduct or evidence of criminality crosses international borders.

5. ARTICLE 4 – TIME PERIODS FOR RETENTION OF DATA

This article provides the basic requirement for the introduction of legislation for the retention of communications data for a minimum of twelve months and a maximum of thirty- six months across all Member States. A minimum retention time period is required as a common rule to improve judicial cooperation in criminal matters.

The article also contains a derogation to allow individual Member States to vary these time periods in certain circumstances with reference to specific technologies not including telephony. These technologies include for example text messaging and e-mail. The retention time periods for these technologies, by electing to use the derogation, can be both increased and decreased by Member States.

6. ARTICLE 5 – ACCESS TO DATA

The purpose of this Article is to take advantage of the instruments on judicial co-operation to which Member States are already parties and that apply to matters within the scope of the Framework Decision. In particular, the Convention for Mutual Legal Assistance in criminal matters among Member States of the European Union, signed on 29 May 2000 (in its Declaration of 26 March 2004, the European Council urged Member States to ratify before the end of 2004).

7. ARTICLE 6 – DATA PROTECTION

This article constitutes a key element of the framework decision, which aims not only to improve the efficiency of our national systems in the fight against crime but also to ensure its compatibility with privacy and data protection principles.

The Article draws from data protection principles described in other EU and international instruments, in particular Directive 95/46/EC. It ensures that consideration is given to the necessity and proportionality of access to the data sought and the need for decisions relating to the access to communications data to be made on a case by case basis in accordance with national law of the individual Member State.

8. ARTICLE 7 – DATA SECURITY

This article relates to the integrity and the ability to ensure continued integrity of the retained communications data. It is essential that communications data be retained to the same standard on the service provider's network throughout the entire period of retention. The Article further provides that the access to such data must be clearly defined in the national law of the individual Member State.

9. ARTICLE 8 – IMPLEMENTATION

This article makes it clear that during the implementation process it will be essential for each Member State to enter into discussions, relating to the provisions of the Framework Decision, with the communication service providers within its jurisdiction.