Non paper
Data Retention

Introduction

At the meeting of the Working Party on co-operation in criminal matters on 4 June a number of delegations expressed concern about the exact kind of data covered by the initiative needed to be clarified.

This non-paper has been prepared by the Presidency [with assistance of law enforcement experts from BEL, DE, DN, FR, NL, POR, SWE, UK] to articulate law enforcement's requirements for historic communications data. The paper provides an interpretation of the scope of data retention that is implied by the 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 (8958/04).

The law enforcement experts reaffirmed the critical value of historic communications data in the prevention, investigation, detection and prosecution of crime and criminal offences including terrorism and expressed support for the aim of the draft Framework Decision to meet the current generic needs of law enforcement.

The frame work decision defines communication data as subscriber data, traffic data and location data. This non paper gives some examples to the traffic and location data. The technical development of the market does not allow for precise or complete descriptions of these data.
Some historic traffic data may require historic information concerning the network configuration to be kept.

The experts reaffirmed that none of the data described in this paper includes any content of any communication.

The scope of traffic data and location data requirement and examples

WHO?

Who (or what) initiated the communication (the "user")?

Source identification, including translated source identification

e.g. E.164 Terminal Address (Calling Party)
ENUM
Subscriber/User number/identifier
Equipment number/identifier
Network Entry Point
IP Address (Static or Dynamic)
PIN number

Who (or what) was communicated with?

Destination identification, including translated destination identification (including intermediate identification)

e.g. E.164 Terminal Address (Called/terminal Party)
ENUM
Subscriber/User number/identifier
Equipment number/identifier
Network Exit Point
IP Address (Static or Dynamic)
TCP Port Number

Who (or what) provided the communication service?

Who (or what) was provided the communication service (the "subscriber")?

WHEN?

When did the communication take place?

Date and time of events, referenced to a public time standard (time zone) and accurate to within 1 second.

When did the communication start/initiate?

Accurate date and time.

When was the communication delivered?

e.g. e-mail, voicemail, MMS, SMS, paging.

When was the communication picked up?

When did the communication end/terminate?

WHERE?

Data necessary to identify the location of devices at the start and throughout the duration of the communication.

e.g. Where did the communication take place?
Where did the communication start from?
Where was the communication made to?

HOW?

How did the communication take place?

Data available on the type of service used.

e.g. Fixed circuit switched service (e.g. PSTN, ISDN, Intelligent Networks, CPS, ISVR)
Mobile circuit switched service (e.g. GSM, IS41, UMTS, S-PCS)
Packet switched service (e.g. X.25, Internet Protocol, VoIP, Satellite)
Streaming data service
Fixed access services for packet and streaming services (e.g. dial-up, Cable, DSL, ISDN D-Channel)
Mobile access services for packet and streaming services (e.g. GPRS, UMTS, TETRA, WLAN)
Trunking service (e.g. MPT 1327, TETRA)
Messaging service (e.g. Paging, SMS, Voicemail, E-Mail, Unified Messaging Services, MMS)
Semi-broadcast service (e.g. Interactive TV)

Data available about how the service was used
Voice, Fax, Data, etc

Was it a successful or unsuccessful communication?

e.g. Connected–effective / connected-ineffective

How was the communication ended?

Release cause e.g. inexplicable termination