Principles on the Availability of Data Essential to Protecting Public Safety

To investigate, so as to prevent or prosecute, crimes and terrorist activities, law enforcement authorities require lawful access to traffic data and subscriber information held by communications service providers. However, criminal and terrorist investigations are increasingly being hampered by a lack of available data and information.

For this reason States should examine their policies concerning the availability of traffic data and subscriber information so that a balance is struck between the protection of privacy, industry's considerations and law enforcement's fulfillment of the public safety mandate. Specifically, in developing a balanced approach, States should uphold human rights, including the protection of personal data. Data protection policies should strike a balance between the protection of personal data, industry's considerations such as network security and fraud prevention, and law enforcement's needs to conduct investigations to combat crime and terrorist activities.

Governments and industry should recognize that the advancement of technology and electronic commerce includes the safety of the public in its use. Ensuring that the public and businesses are safe and secure is essential for the continued health of national economies and the growth of consumer confidence in doing business on the Internet.

In order to facilitate a balanced approach when developing policies regarding the availability of traffic data and subscriber information, consultations should be conducted with all relevant stakeholders including data protection and privacy authorities, industry, law enforcement agencies and users.

Governments and industry should recognize that there are economic implications to the collection and retention of data, which are dependent on a number of factors including the amount of available data (e.g., which fields in which logs), the time period for storage, and different business modules. Therefore, governments should specify the types of data that would be useful for public safety purposes. Some logs, for example network access logs, are particularly useful for lawful investigations. Annex A contains a list of logs that may be available.

Governments should seek to avoid unreasonable operational and financial burdens on different ISP business models with respect to ensuring the availability of traffic data and subscriber information.

States should develop cooperative approaches regarding the availability of data in order to avoid undue burden on service providers that supply services across borders, taking into account any applicable international trade obligations.

Policies developed at the domestic level regarding the availability of traffic data and subscriber information should take into account the need for international cooperation to enable the rapid tracing of**ck to Introducti**

G8 Justice and Interior Ministerial, May 2002

criminal and terrorist networked communications across national borders.

Annex A

The following is a list of log details related to some services that may be available to an Internet service provider. It should be noted that the content of these logs might be subject to relevant business, technical and legal conditions; not all of the following data elements will be available in all logs.

(1) Network Access Systems (NAS)

- access logs specific to authentication and authorization servers such as TACAS+ or RADIUS (Remote Authentication Dial in User Service) used to control access to IP routers or network access servers
    - date and time of connection of client to server[(1)]
    - userid
    - assigned IP address
    - NAS IP address
    - number of bytes transmitted and received
    - caller Line Identification (CLI[(2)]).

(2) E-mail servers

- SMTP (Simple Mail Transfer Protocol) log
    - date and time of connection of client to server
    - IP address of sending computer
    - ID Message (msgid)
    - sender (login@domain)
    - receiver (login@domain)
    - status indicator
- POP (Post Office Protocol) log or IMAP (Internet Message Access Protocol) log
    - date and time of connection of client to server
    - IP address of client connected to server

- userid
- In some cases identifying information of E-mail retrieved

(3) File upload and download servers

- FTP (File Transfer Protocol) log
  - date and time of connection of client to server
  - IP source address
  - userid
  - path and filename of data object uploaded or downloaded

(4) Web servers

- HTTP (HyperText Transfer Protocol) log
  - date and time of connection of client to server
  - IP source address
  - operation (i.e., GET command)
  - path of the operation (to retrieve html page or image file)
  - "last visited page"
  - response codes

(5) Usenet

- NNTP (Network News Transfer Protocol) log
  - date and time of connection of client to server
  - protocol process ID (nnrpd[NNN……N])
  - hostname (DNS name of assigned dynamic IP address)
  - basic client activity (no content)
  - posted message ID

(6) Internet Relay Chat

- IRC log

G8 Justice and Interior Ministerial, May 2002

- date and time of connection of client to server
- duration of session
- nickname used during IRC connection
- hostname and/or IP address

[1] Reliable time records among different computers and networks is essential for investigation and prosecution. The use of the Network Time Protocol (NTP) for synchronization should be an ISP Best Practice. [2] CLI provides the number from which a telephone call is made and may or may not be available to ISPs. CLI retrieval is specific to the given combination of software and hardware. See "LINX Best Current Practice - Traceability", section 10.2.