Data Retention vs Data Privacy

By Therese Saliba Khairallah
Operations Manager
Inconet Data Management SAL
E-mail: therese.saliba@idm.net.lb

Middle East Cyber Crime Forum
Beirut, Lebanon, 23rd & 24th February 2006

IDM
IncoNet - Data Management

Agenda

- Data Retention principles & issues
- Current Practices relating to Data Retention
- Global Debates
- Implications
- Thoughts

IDM
IncoNet - Data Management

Data Retention principles & issues

Data Retention Types

- **Information contained in a Log File, related to End-User's identity, location, destination,…**
- **Content of Communication: emails, chat, web pages downloaded, voice over IP communication, video communication, peer-to-peer communication (Napster, Kazaa, Morpheus, iMesh etc…)**

Not dealt with in the following presentation

Data Retention Process

- **Data Collection**
- **Data Storage**
- **Data Retrieval**

IDM
IncoNet - Data Management

Data Retention principles & issues

Data Collection

- **Data collected from Switches, Routers & Network elements**
  - Authentication Data
  - IP Assignments, IP Flow Logs
  - Routing tables
  - Syslog data, snmp data
- **Data collected from: Servers, Service Gateways**
  - DNS servers
  - Mail servers (smtp, pop, ..)
  - Web & FTP Servers
  - Cache Engines, Proxy, NAT etc…
- **Data collected from: Databases**
  - User Data (name, address) & Billing information

Time stamp collected from all the above

IDM
IncoNet-Data Management

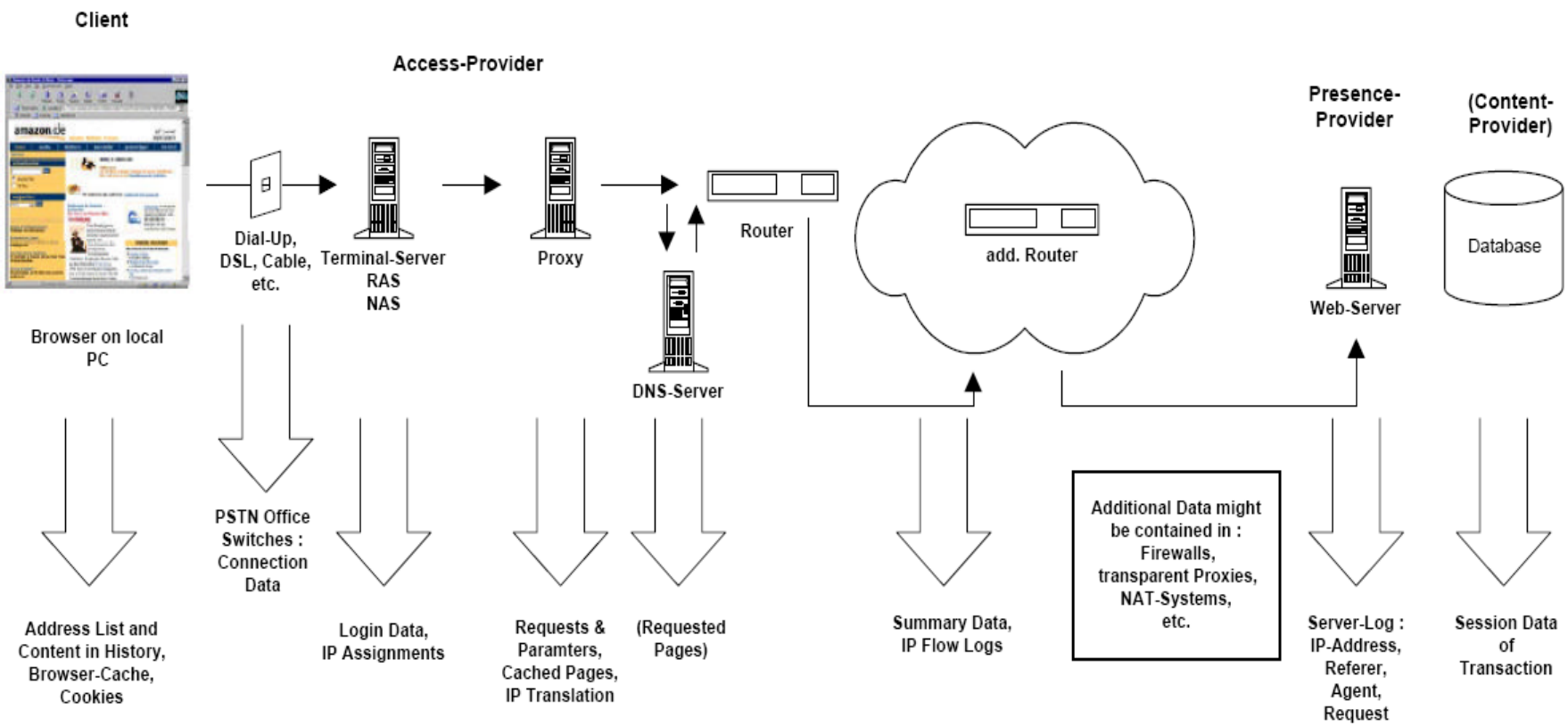
Data Retention principles & issues

Data Collection (Cnt'd)

- **Possible Data to log at the access Provider level**
  - Login Data & IP assignments at the terminal server level
  - Requests & parameters, cached pages, IP translation at the proxy level
  - Requested pages at the DNS level
  - IP Flow logs at the router and switches level
  - Additional data in log files from Firewalls, transparent proxies, NAT systems, intrusion Detection etc…
  - Operating System Access (i.e. High level administrative or root access)
  - Application access (i.e. users and objects with write and execute privileges)
- **Possible Data to log at the Presence Provider level**
  - IP-Address
  - Requested page

IDM
IncoNet-Data Management

Data Retention principles & issues



IDM
IncoNet-Data Management

Data Retention principles & issues

Data Collection: Issues

- **Data collected from Switches, Routers & Network elements**
  - No single point of collection for the whole network
  - Same data logged several times in Network
  - Data provided is raw data, pre-processing required to produce useful, readable data
  - Information required to produce useful logs require outside sources (i.e. DNS, other Providers)
- **Data collected from: Servers, Service Gateways**
  - Multiple Log Files formats, plain text
  - Huge amounts of data, dependant on log detail level
  - Log Files designed for humans, not easily machine readable
  - Anonymous use often possible
  - High probability of source being intermediary (Proxy, NAT, load balancing)

IDM
IncoNet-Data Management

Data Retention principles & issues

Data Storage

- **Data storage situation**
  - Long-Term storage only for billing records
  - Secure storage of logs is not an industry standard practice
  - Separate storage required for on line and off line data
- **Data Storage: Issues**
  - Storage of raw data will not lead to useful information
  - Storage of preprocessed data requires significant processing
  - Long-Term Retention of data means massive volumes of data (TB) depending on:
    - ISP Size
    - ISP Service Portfolio
    - Number of Subscribers
    - Subscriber's Consumption Volume (Note: Introduction of ADSL promotes large video transfers)

IDM
IncoNet-Data Management

Data Retention principles & issues

Data Retrieval

- Internal resources needed to handle requests for Data
- Separate and powerful systems to search for data quickly
- Development of new retrieval systems to cope with ISP regularly changing systems:
  - ISPs would require highly qualified staff to insure the development or the maintenance of such systems
- Availability of intelligent software for data retrieval worldwide

IDM
IncoNet - Data Management

Current Practices relating to Data Retention

Current Logging

- **Currently ISPs can log the following from Several Sources Manually:**
  - IP Address – Assigned by ISP to a user
  - Telephone Line a username is using – Dial-up Users (Availability of Digital Lines)
  - Location of the Hotspot a username is using – WIFI Users
  - Duration of Connection – (Start Time / Stop Time) for all users using authentication data to connect
  - ISP Mail Application – From / To, IP, Time Stamp, sent or not, received or not
  - Website Visits (URLs) from Cache Engines (Date, IP, URLs, Time Stamp)

IDM
IncoNet-Data Management

Current Practices relating to Data retention

Issues with current practices

- **Difficulty to know the username ID in the following cases:**
  - **prepaid card bought from the market**
  - **IP assigned to a public internet access (Internet cafe)**
  - **IP assigned to an enterprise providing Internet access to its employees**
  - **IP assigned to an educational institution providing access to its students**
  - **IP assigned to a roaming user**
- **Duration of retention is variable from years to minutes, depending on the logged data and the ISP**
- **ISPs start retaining less and less data due to unlimited usage provided now and due to the increasing amount of retained data.**
- **Unclear Data privacy law in Lebanon (Lebanese citizens rights)**

IDM
IncoNet - Data Management

Current Practices relating to Data retention

Scenarios of Government Requests Fulfilled by ISPs Today.

- **Case 1: tracking the identity of an IP address (case of an IP address implicated in a cyber crime)**
- **Case 2: tracking usage from a certain telephone line (case of a customer refusing to pay the MOT bill, denying using the Internet)**
- **Case 3: tracking the initiator of an ISP e-mail: IP address, telephone line (case of business e-mails read by a spy)**
- **Case 4: tracking username caller id (case of stolen computer)**

IDM
IncoNet - Data Management

Current Practices relating to Data retention

Process of requests coming today to ISP

- **Request to the ISP from Internal Security Forces approved by the Public Prosecutor before the Supreme Court**
- **ISP will fetch in the Log Files**
- **ISP will send an official letter to the Internal Security Forces in answer of the request with the results**

IDM
IncoNet-Data Management

Global Debates

- **EuroISPA – European Internet Service Provider Association**
  - Mandatory law for data retention for two years, but still debated
- **USISPA – United States Internet Service Provider Association**
  - No mandatory law for data retention but they share most of EuroISPA concerns
- **ARISPA – Arabic Internet Service Provider Association**
  - Just starting
- **AFRISPA – African Internet Service Provider Association**
  - No info on data retention law on their web site

IDM
IncoNet - Data Management

Implications

- **ISPs**
  - Additional very high cost, new innovative services, competition, high quality of services
- **End-User**
  - Cost, Privacy, flexibility (to use the service from a network café, hotspot, prepaid cards, online buying, future vending machines…)
- **Government**
  - Additional cost to reimburse the ISP's in case of a mandatory law of retention
- **Risk on some Type of Business**
  - E-commerce

IDM
IncoNet-Data Management

Implications – Cost Factors

- Network design of the ISP and its size
- Number of Subscribers
- Service portfolio
- Duration of Retention Regime
- Which data falls within the retention regime
- Quality of Data (i.e. must it be of evidential quality?)
- Highly Skilled people for dealing with requests
- Attending Court Cases
- Maintaining “Golden Copies” of data passed over to law enforcement authorities
- Hardware & Software infrastructure for the retention required
- Upgrade of existing Hardware for logging
- Highly skilled people to maintain the intelligence of retention
- Global Time Synchronization

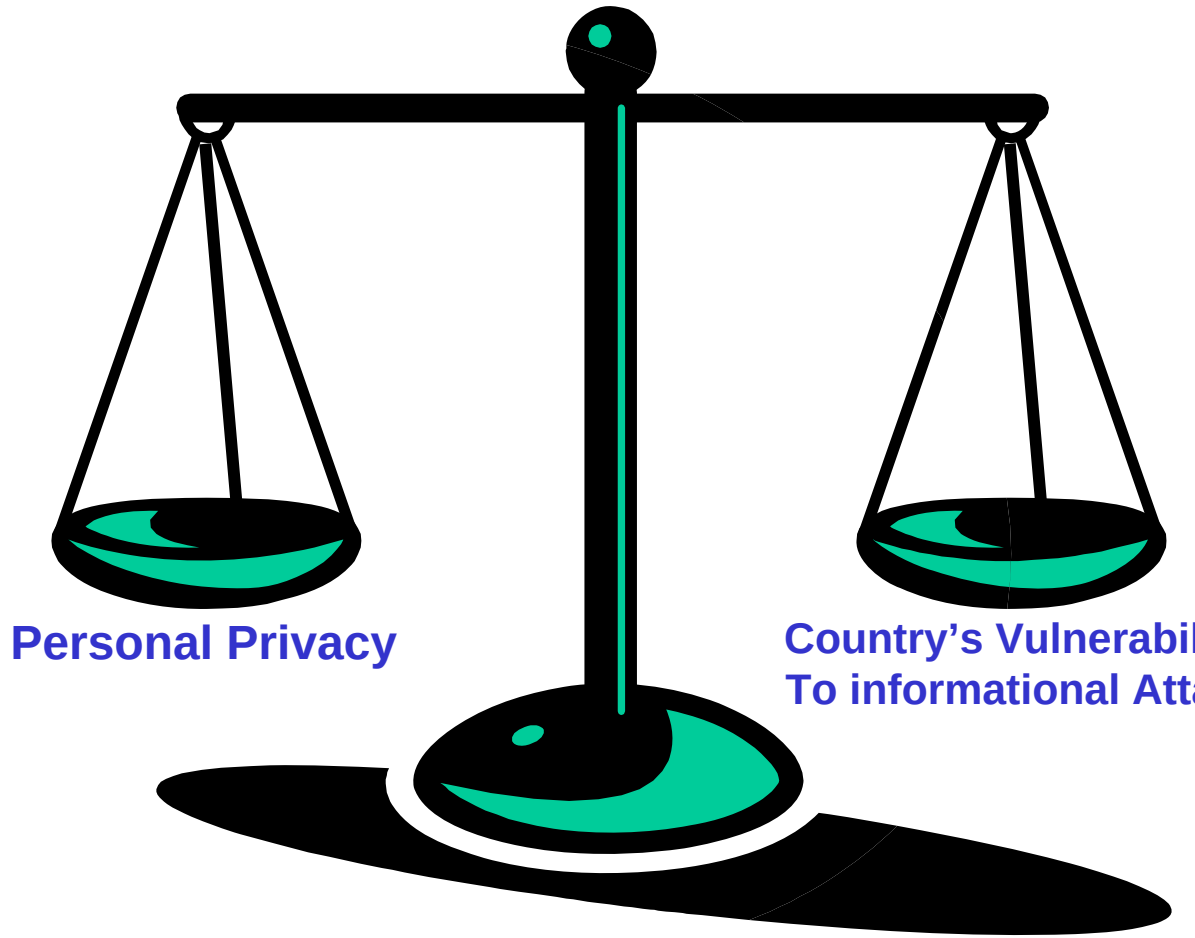
IDM
IncoNet-Data Management

Thoughts

- End-User Privacy versus Government Security
- Data protection and data retention requirements are almost mutually exclusive
- Data retention is a potential infringement of fundamental rights and laws in the country
- A Sustained period of close dialogue between the relevant stakeholders (Government, ISPs, Legislators, Regulators)
  - Qualified Department in the Government to maintain this dialogue
  - Establish a framework to provide ongoing industry input

IDM
IncoNet-Data Management

Data Privacy & Security



IDM
IncoNet-Data Management

Data retention vs Data Privacy

Thank you for your attention

By Therese Saliba Khairallah
Operations Manager
Inconet Data Management SAL
E-mail: therese.saliba@idm.net.lb

Middle East Cyber Crime Forum
Beirut, Lebanon, 23rd & 24th February 2006

IDM
IncoNet - Data Management