EU Data Retention
- Recent Developments -

22C3 Congress
Berlin
27.12.2005

Why are we here?

- In the information age, a significant portion of communication takes place through electronic means.
- Law enforcement considers insight into the communication process an essential source for investigations
- For investigation purposes, the actual content of a communication is only a secondary consideration. Most prominent is the question:

Who communicated with whom at what point in time?

A short history of Data Retention I

Draft Framework Decision introduced by UK, Ireland, Sweden, France on April 28th 2004

- Massive demands: Traffic Data for all types of communication and protocols
- Data to be stored for 36 month
- Data for unsuccessful calls, routing information etc. is to be stored as well.

A short history of Data Retention II

After consultation with industry in June 2004 and a feasibility study in August 2004, the Dutch Presidency releases an amended draft on October 14th, 2004

- Some improvements, most notably a 12 month period and a more realistic view on data types

A short history of Data Retention III

- No movement during the Luxembourg Presidency
- In June 2005, the EU parliament rejects data retention based on the Alvaro report:
  - 180 million Euros per year burden on every large telco in Europe, Internet service providers face threat to their existence
  - Incompatible with the European Convention on Human Rights
  - No visible benefits, not even the police wants it

A short history of Data Retention IV

- UK takes over the presidency on July 1st 2005
- London tube bombings on July 7th 2005
- Charles Clarke makes it a personal priority to implement harmonized Data Retention
- New council position paper released July 27th 2005
- On September 8/9th 2005, joint meeting of Interior&Justice Ministers in Newcastle. Presentations by Industry, but no progress.

Political Impact Assessment

- No legal basis for a framework decision by the council, 3rd pillar instrument deemed insufficient.
- Significant concerns raised by Data Protection officials
- Extreme cost of up to several billon EUR can/will not be shouldered by some states.
- Still, council demands a decision by end of 2005

The Commission proposal

- To overcome the legal deadlock, the EU Commission released a “Proposal for a Directive” (a 1st Pillar instrument) on September 29th, 2005.
- While in principal based on the Council text, it holds significant improvements over the Council text.
- Most notably, countries would have to reimburse the full cost of Data Retention to the industry.
- There are no mechanisms provided to control the use of Data, an extension of Data types to be stored can be implemented the simple change of an annex.

Existing legislation

- Some countries have adopted measures already, i.e. Ireland, Italy, France.
- Some countries developed a split between the parliament position and the government view, i.e. Germany, UK, Netherlands
- Some countries refuse Data Retention altogether, i.e. Austria, Finland

Role-Playing the EU parliament

- Council rejects the Commission proposal on October 10th , cost being the most significant concern. A “joint” commission/council proposal is released on November 29th 2005
- Without consultation, heads of socialist delegation and conservative delegation agree a text with Charles Clarke, released December 2nd 2005
- Despite unanimous protests by various groups, EU parliament votes in favour of the compromise on December 14th 2005
- Even EU parliament amendments are not considered, Alexander Alvaro withdraws his report and name

The de-facto situation today

- Data Retention has been agreed by parliament and member states as a Directive
- The text adopted will require retention to be implemented in all European countries
- It is doubtful that the text will be upheld by EUGH
- It is very likely that the measure will be deemed incompatible with fundamental rights in at least one EU member state

What's in the resolution?

- "Only" concerns storage of user, traffic and location data which is "generated or processed" for 6 to 24 month (but countries can file for more or less)
- Can only be used for "serious crimes", but up to the countries national law which crimes are serious
- Rules to access the data is "to be defined in national law"
- No content data whatsoever:
  "No data revealing the content of the communication can be retained pursuant to this directive" (Art. 4, 2)

Categories of Data to be retained I

Data necessary to trace and identify the source of a communication:

…

Concerning Internet Access, Internet e-Mail and Internet Telephony:

- The User ID(s) allocated
- The User ID and telephone number allocated to any communication entering the public telephone network
- Name and Address of the subscriber or registered user to whom an IP Address, User ID or telephone number was allocated at the time of the communication

Categories of Data to be retained II

Data necessary identify the destination of a communication:

…

Concerning Internet e-Mail and Internet Telephony:

- The User ID or telephone number of the intended recipient(s) of an internet telephony call
- Name(s) and Address(es) of the subscriber(s) or registered user(s) and User ID of the intended recipient of the communication

Categories of Data to be retained III

Data necessary to identify the date, time and duration of a communication:

…

Concerning Internet Access, Internet e-Mail and Internet Telephony:

- The date and time of the log-in and log-off of the Internet access service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access provider to a communication, and the User ID of the subscriber or register user.
- The date and time of the log-in and log-off of the Internet e-mail Service or Internet telephony service based on a certain time zone

Categories of Data to be retained IV

Data necessary to identify the type of communication:

…

Concerning Internet e-Mail and Internet Telephony:

- The Internet service used

Categories of Data to be retained V

Data necessary to identify users communication equipment or what purports to be their equipment:

…

Concerning Internet Access, Internet e-Mail and Internet Telephony:

- The calling telephone number for dial-up access
- The digital subscriber line (DSL) or other end-point of the originator of a communication
- … (?!?)

International comparison

- Basis for measure is the “fight against terrorism”
- US Agencies see no advantage of Data Retention over Fast Freeze, no proposals today
- Israel considers personal rights the higher good, no Data Retention proposals today
- Ireland will enact legal action (no harmonisation, timeframes to low)
- France has just adopted a new police law which requires no court order to access the data
- Poland aims for 15 years of data retention

The human rights issue

- Parliaments throughout Europe have rejected Data Retention in the past
- Data Protection officials reject the proposal as incompatible with existing legislation:
  - All communication data of EU citizens will be stored, independent of a specific investigation
  - The fundamental right of privacy in communication will be violated

Factual Analysis I

- Law enforcement could never demonstrate the effectiveness of data retention over alternatives, i.e. Fast Freeze/Quick Thaw
- Throughout the process, law enforcement did only name three (!) cases where historic data helped solve a case
- There is no concept for the processing of Internet Data, it has also become clear that there is no awareness of the problems involved or the situation “on the street” today (i.e. public access)
- User might not even be aware of his communications (i.e. automated processes, spam, DOS), no validation or authentication provided

Factual Analysis II

- Methods used by home affairs are highly questionable for a public process, discussions were generally avoided or stopped dead by the “responsibility” argument
- Commission “blackmailed” by the Council: Adoption of the joint text demanded within 2005 in order to avoid an independent council framework decision
- Normal Commission consultation process not possible
- Many governments demanding Data Retention have no mandate by their parliaments

What does it mean for industry?

- Complete paradigm shift: Store as much as you can, not as little as you can
- Cost impact varies significantly depending on country, no harmonization at all
- Procedures & Processing capabilities for correlating usage data with administrative data required
- Measure requires secure, reliable storage systems, operated separately in order to uphold data protection rules – not industry standard for log files
- Dedicated personal required, access without “undue delays” need to be ensured (analog to legal interception)

Technical Analysis – Acquisition

- Multi-level data retrieval, routers, hosts, admin systems
- Significant portions so far never systematically retrieved and stored, i.e. IP flow data correlated with user data
- Will require significant system upgrades due to load issues
- New investments in end-of-life technology required (i.e. SDH/SS7)
- Significantly more flows in data networks (several orders of magnitude over classical voice)

Technical Analysis - Processing

- In the Internet space there will potentially be thousands of connections per session, which need immediate pre-processing in order to become useful at all.
- Data types not adequately defined or data not available to providers (i.e. source and destination of a communication)
- Cost of pre-processing (industry) vs. cost of post-processing (law enforcement) vs. response time

Sanity check

- Data not usable on an individual base, even if pre-processed – need multiple sources to overlay
- Unclear how to detect and store VoIP – concept of "real world" VoIP networks flawed even at regulatory offices
- Unclear how to uphold certain requirements, i.e. BCC: of emails
- Certain details possible and probably O.K., i.e. IP/user mapping over time IMHO not a critical issue

Easy Avoidance Strategies

- No storage if mail server outside EU
- No storage if SIP server outside EU
- No storage if non-standard protocol/port
- Run your own servers/networks, only use public lookup (DNS/ENUM)
- Communications will be stored, but no correlation to user at
  - Internet cafes
  - Public Hotspots
  - Foreign SIM Cards

National Issues - Germany

- Good chance that BVG will overturn resolution
- Parliament resolution from early 2004 ignored by the Government in EU proceedings
- Cost to be fully borne by industry (!) (Schaeuble: “Staatsbuergerpflicht) , only cost individually attributable to retrieval will be partially reimbursed (analog “TKÜV”, however even in legal interception cost issue unsolved since 2004!)
- **To early to tell, first drafts need to be looked at** (released by BMWA, exp. Q2/06)

Conclusions

- Only uninformed individuals can be detected
- Law enforcement has no capabilities to process data provided, even so it is now significantly less data
- States can not afford what they demand, cost will – in the end – be borne by users
- Despite claims to the contrary by home affairs, the measure is grossly disproportionate – but courts will tell.
- The basic principle of police work is overturned: everyone is under investigation all the time

Thank you for your attention

Klaus Landefeld
eco Verband der deutschen Internetwirtschaft e.V.
Lichtstrasse 43h
50825 Köln
klaus.landefeld@eco.de