



thusTM

Thus plc

ISPs, Telcos & Customers

A common view of Data Retention ?

Richard Clayton

Consultant Internet Expert

richard.clayton@thus.net

SCL, London: 29 April 2003



Outline

- **What is an ISP?**
- **What data does an ISP keep and why?**
- **Who are APIG?**
- **Access to communications data**
- **ATCS — an unworkable law?**
- **APIG's view of ATCS**
- **Conclusions**

What exactly is an ISP?

- Internet Service Providers provide connectivity and MAY provide other services such as email, web hosting, file distribution, etc etc
- They are NOT
 - regulators or law enforcement
 - subject to foreign laws
- They have obligations to
 - users - confidentiality
 - users - data protection
 - courts - injunctions, court orders
 - police - warrants etc

What data does an ISP keep and why ?

- **ISPs will record usage**
 - of connectivity
 - of email services (to, from, size)
 - of uploading files
- **Data is kept for business purposes**
 - to settle disputes
 - to track spammers
 - to debug failing systems
- **Telcos keep similar information for these reasons and also (at present) for billing purposes**

What about “web logs”?

- Website logs mainly owned by customers
 - deletion policy under customer control
 - logs can be BIG so pressure to delete
- Web “proxy caches”
 - in principle will indicate which pages were accessed
 - but not universal (and usage may be optional)
 - HTTPS (secure access) will bypass cache
 - the logs are **E N O R M O U S** so records are kept for hours not days (if indeed the logging is switched on at all)

How long is communications data kept?

- **EU Data Protection Directive 95/46/EC**
 - personal data must be deleted when not needed any more for business purposes
- **EU Telecomms Privacy Directive 97/66/EC**
 - call data must be deleted when no longer needed for billing
 - similar wording in upcoming 2002/58/EC
- **Most data gone within a month or three**
- **Data Retention regimes being promoted by some elements of the police, but costs are high and opposition substantial**

Investigative access to comms data

- Large telcos provide it via online links
 - also “special services” at higher cost
- ISPs finally insisting on paperwork
 - growing concerns about data protection & confidentiality issues
 - cost of providing data is becoming significant
- LEAs are still using DPA 29(3) loophole
 - self-authorized RIP s22 notice from police
 - adding other authorities very controversial
- But other authorities have their own Acts

All Party Internet Group

- **MPs and Peers from all parties**
 - **Brian White, Richard Allen & Lord Northesk**
- **If you hold an inquiry then they will come!**
- **Written submissions from industry, FIPR, individuals, Home Office & UK Law Enforcement**
- **Oral evidence in December**
 - **plus a very frank private session with industry!**
- **Report published end of January**
 - **<http://www.apig.org.uk/publications.htm>**

APIG: Access to communications data

- **APIG report deferred to consultation**
- **BUT recommended consulting on:**
 - **better definitions for comms data**
 - **special rules for “predictive” access**
- **Recommended RIP brought into force ASAP**
 - **but after results of consultation clear**
- **Guidance needed on Subject Data Access requests when records show LEA access**
 - **Information Commissioner to advise?**

APIG: Single Points of Contact

- **SPoCs provide a skilled and knowledgeable interface between LEAs & industry**
 - All police forces have one (Met has three!)
- **SPoC scheme fully endorsed by APIG**
 - seen as essential for any new authorities
- **Need clearing house for low volume users**
 - BUT this would require legislation
 - Regulatory Reform Order appropriate?
- **But upper limits on size**
 - prevent institutional abuse

APIG: Legacy legislation etc

- Recommended that access to communications data should be “ring fenced”
 - short term memorandum of understanding
 - primary legislation could be very brief
 - concern about “statutory gateways”

APIG: Oversight

- **Interception Commissioner is responsible for all of Part I (and Part III) of the Act**
 - requested a statement on resources
- **Suggested a SPoC for Commissioners !**
- **Recommended an explicit offence be created for the abuse of the powers in Part I Chapter II**
 - found in HO consultation as a “may” but press briefings suggested that it will happen!

ATCS Part 11 — “emergency legislation”

- Home Office to create Code of Practice for voluntary data retention
- If voluntary fails then can be made compulsory
 - sunset clause effective December 2003
- Industry split on compulsion
 - originally issues of competition
 - now it is legal issues predominating
- No consensus on expense involved
 - time periods unclear & costs non-linear
- Not helped by LEA “Business Case” fiasco

ATCS Part 11 legality

- Parliament amended Bill so retention was only for reasons related to “national security”
- But data access will be under the RIP regime
 - AND legacy legislation AND civil action
- This creates a “disparity” issue
 - retention of the data is lawful
 - but access might not be HRA compliant
- Parliament has deemed retention to be “proportionate” just for national security
 - and not, by implication, for general crime
 - and some argue they’re mistaken anyway

APIG: Part 11 conclusions

- Industry is concerned that a voluntary scheme would expose them to action under HRA (because they are acting as a public authority)
- Plus issues of cost in post-dotCom world
- Pretty clear that voluntary scheme is doomed
- High costs remain an issue if compulsory
 - telcos might well take systems abroad
- APIG recommended forgetting ATCS and going for US style “Data Preservation” instead
 - but Home Office pressing on for now...

APIG: oddments

- **Collect statistics on usage of comms data**
 - no-one knows how much is currently used (though Simon Watkin has some best guesses)
- **Review overall use of comms data in longer term**
 - Internet “connections” meaningless in a broadband society!
- **LEAs and industry should continue to co-operate**
 - motherhood and apple pie!
 - but in some countries it wouldn't be!
- **Annual Parliamentary debate on privacy**

Conclusions

- **APIG report is required background reading**
 - concise summary of complex area
 - <http://www.apig.org.uk/publications.htm>
- **Did not have much effect on consultation paper**
 - and even less on Home Office policy
 - but has helped to inform debate
- **The ATCS debacle^W debate is far from over**
 - s122 report of privy councillors
- **and we still have RIP Part III to come.....**



thus™