Communications Data Bill

UKNOF 23 – October 2012

Zoe O’Connell

Communications Data Bill

- The Current Situation
- The Problem
- Home Office Solution: The draft Communications Data Bill
- Impact on Service Providers
- Where to now? (The political bit)

Current Situation

- Interception
  - Regulation of Investigatory Powers Act 2000, section 5 warrant
    - These are secret and require a warrant issued by the Home Secretary
- Storage
  - The Data Retention (EC Directive) Regulations 2009, s.10 notice
    - Sent by the Home Office to large Service Providers, so date can later be disclosed
- Disclosure
  - **Criminal:** Regulation of Investigatory Powers Act 2000, s.22 notice
    - Routine, issued by police and others - Over half a million per year
    - Most Service Providers will have seen at least one of these
  - **Civil:** Court orders
    - US court orders not valid!

The Problem

- 25% of data is “unavailable”
  - This has been largely attributed to ambiguities in the Data Retention Directive
- The security services want more data
  - They are willing to spend large amounts of money on this: £1.8 billion over 10 years, over half of which will be spend on storage
- Beyond that, they are vague
  - This is being lead by the security services, not the police

The Home Office Solution

Interception Modernisation Programme (IMP)

…which was dropped by Labour and post-2010 became the…

Communications Capability Development Programme (CCDP)

…leading to the announcement in the Queen's speech of the…

Communications Data Bill (CDB)

…which then became the…

Draft Communications Data Bill

The Home Office Solution: Interception

- Part 1 grants nearly unlimited power to the Home Secretary to mandate interception
  - Will only cover communications data, not content.
  - Equipment and configuration to be used will be specified by Home Office.
  - Technical details are not forthcoming, but encryption is “not a problem”.

The Home Office Solution: Storage

- As well as interception in transit, service providers (e.g. Facebook, Twitter) will be required to store more data
  - This is effectively an extension of the EU Data Retention Directive
  - Data will be stored at the service provider, not centrally by the Home Office.

The Home Office Solution: Disclosure I

- Disclosure will function much as the existing system
  - The Home Office will not have direct access to black box data and still need to request it from the service provider
    - But automated filtering of data permitted. For example, a Service Provider may have to hand over everything, so the Home Office can filter it themselves.
- Fewer organisations will initially have access: Security Services, SOCA/NCA, Police, HMRC.
  - This can be expanded by secondary legislation to anyone.

The Home Office Solution: Disclosure II

- The Home Office intent to cooperate with foreign service providers, rather than use interception
  - The legal basis for this is unclear

Impact on Service Providers: What Service Providers are saying

- **The Home Office**: Service Providers in private conversation have said they understand what is required of them and are OK with this.
- **The Bill Committee**: Service Providers have given public evidence under oath stating the opposite.
- It is likely nobody really fully understands any potention impact at this stage.
  - The Home Office know what they want and how they think they can do it.
  - The technical folk at Service Providers know what is possible.
  - The Home Office will not tell the technical folk anything.

Impact on Service Providers: Interception I

- Will you be affected by interception changes?
  - The Home Office have publicly stated their focus is on cooperation and storage, not interception
  - If you have **no international circuits**, it seems unlikely you will be required to host black boxes.
  - If you **do have international connections**, and are large enough to come to the notice of the Home Office, expect black boxes.
    - Or simply more black boxes on every connection, for those that already have them.

Impact on Service Providers: Interception II

- Operational Impact?
  - Active vs. passive interception
    - Will active modification of the data stream be required – e.g. Man-in-the-Middle SSL attacks?
    - Will only “interesting” data be run through the system, similar to Cleanfeed?
  - Sitting in the middle vs. port mirroring
    - Detection of link loss, UDLD, BFD etc.
  - Upgrades will become harder
    - Suddenly that proposal to add another 1Gb/s link needs Home Office approval

Impact on Service Providers: Storage

- If you can generate and store it, expect to be asked to.
  - Use of Drafts folder to store communications.
  - “Three Lions” film – terrorists used a kids penguin game to chat.
- Operational impact?
  - More storage.
  - More bandwidth.
  - More money.
  - Just another project, but guaranteeing you have wiped all data can be tricky.
    - (As long as you are not asked to store data from client virtual servers/web sites!)

Impact on Service Providers: Disclosure I

- Intercepted data
  - Hopefully well documented mechanisms would exist for retrieving data from Home Office equipment.
    - Lower training requirement for SPs that are not large enough to have a dedicated abuse & compliance team
- Stored data
  - Should be easier, as dedicated systems for data collection rather than querying operational systems.
    - (But this depends on how well you build the system!)
- Likely changes in SPOC system
  - Mid-to-large providers more likely to have formal contact with the Home Office, so no more s22 notices arriving at your offshore support centres.
  - Smaller providers may be left (even more) out in the cold

Impact on Service Providers: Disclosure II

- Twitter: “Legally untenable position” for foreign providers
  - Likely to result in the retention and perhaps disclosure of non-UK users data.
  - This may breach laws or terms of service in other countries.
  - Grey area where users travel between countries.
- Direct operational impact of this likely to be minimal
  - Legal implications of getting it wrong could be significant.
    - How good is your Geo-IP data?
    - Foreign Service Providers will likely get funding for storage, but not for figuring out complicated legal situations!

Where to now?

- Parliamentary Joint Committee established to study the draft bill
  - Mixed membership
    - 5 Conservatives (3 MPs/2 Lords), 4 Labour (2/2), 2 Liberal Democrat (1/1), 1 crossbench Lord.
  - Has heard oral and written evidence from Home Office, service providers and other interested groups
    - Security Services unused to scrutiny and did not do a good job in evidence.
  - Committee will report later this year (October/November)
    - Likely to say: “You’ve got the language wrong, you’ve got the whole concept wrong, you have to start again… So I think that will kill this bill”.
- Unlikely to pass Commons during this parliament, due to “The Huppert Veto”.

THANK YOU