Network Security 22: The Law

i.g.batten@bham.ac.uk

UK/EU Centric

- European Convention on Human Rights
- European Data Protection Directive
  - Transposed into most EU members
- European Data Retention Direction
  - Ditto
- Most countries have laws like our Regulation of Investigatory Powers 2000 legislation and the (as yet untested) Investigatory Powers 2016 which came into force at the end of 2016.

Basic Rights

Article 8 – Right to respect for private and family life

1. **Everyone has the right to respect for his private and family life, his home and his correspondence.**

2. There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law and** is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

UK Law

- ECHR now adopted into UK law by Human Rights Act 1998
- Even if we abolished that, we would still be signatories to the ECHR.
- Not related to the EU: leaving the ECHR much more serious, as would involve leaving Council of Europe.
    - But in the current febrile climate, who knows?

IOCA 1985

- Historically, interception was done on a “nod and a wink” basis. All telecoms controlled by government (GPO) so police and agencies just spoke to their fellow civil servants. Regulation honoured more in the breach.
- Interception of Communications Act 1985 introduced when GPO privatised and OLOs started to appear (Mercury, initially)
  - Put interception on a statutory footing.

Be down with telecoms kids

- LO: licensed operators (usually taken to mean big incumbents)
- OLOs: other licensed operators
- MOLOs: mobile licensed operators.
- In the US, ILEC (incumbent local exchange carrier) and CLEC (competitive local exchange carrier) roughly equivalent to LO and OLO.
- In UK, competitive local carriers may or may not offer voice: SMPF (Shared Metallic Path Facility) means you can be connected to Talk Talk's DSLAM but BT's voice facility.

Case Law

- Halford v. United Kingdom , (20605/92) [1997] ECHR 32 (25 June 1997)
  - Police used powers of interception to listen to communications between employee and her lawyer, prior to industrial tribunal case on sex discrimination
  - ECtHR gave right of privacy to certain calls made on business premises

Data Protection Act 1998

- Imposed obligations on fair processing (not part of this course)
- But Seventh Data Protection Principle applies:
  - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

RIPA 2000

- Regulation of Investigatory Powers Act 2000
- Response to Halford case, and other events
- I'm biased for reasons I will explain, but I think it is basically sound legislation
- Accusations of being "snoopers' charter" forget that prior to RIPA all this stuff was just done anyway
- Never about terrorism: about entire intercept regime, to balance Article 8 rights with IOCA capabilities.

RIPA CoP

- Provides extensive guidance on what you can do on your own networks if you are not a telecoms operator.
- Limited case law.
- Halford issues over private phonecalls (etc) rendered moot by mobiles
- Subject to notification, you can pretty much look at anything you want

RIPA in Enterprise

- Public sector organisations tend to err on side of caution, and are wise to have internal approval system for access to employee/student data
- Private sector tends to say “our wires, our bits” (and puts that in contracts of employment)
- There will be complex case law over BYOD (see last lecture) because it’s not obvious what is “our wires” in that context: be prepared for excitement.

RIPA/IPA in operators

- Operators should not look at content without reasonable cause (essentially, without a warrant)
  - Not clear that an offence is actually committed, as RIPA is all about government powers, not citizen protection, but common-law duties of confidence probably apply
  - If an operator looks at your packets, what happens?
- Distinction for warrants between communications data and content

Communications Data

- Headers, envelopes, logging, billing…everything that isn't the actual content of the communication
- Available to police, agencies and a cast of thousands (the Egg Marketing Board!) over the signature of a senior officer.
    - Single Point of Contact regime should be followed
- Mostly (until recently almost exclusively) reverse DQ

Content Data

- Requires warrant personally signed by minister
  - Home Secretary for most cases, Foreign Secretary for GCHQ work not affecting UK citizens
- Worth noting: nothing in Snowden revelations suggests policy is being broken, but much evidence that they are sailing very close to the wind
  - Question: is it OK to intercept a whole feed, filter with a computer and get a warrant for the output? Currently, probably yes, but this is at the heart of the debate about bulk collection. Case law is needed.

Responsibility

- Contrary to popular belief, operators are not responsible for data on their networks, nor are enterprises, with some very narrow exceptions
  - Sexual Offences Act provides some protection for enterprises
- Running open WiFi is perfectly OK
- Salesmen love to say otherwise
- Very narrow list of “illegal to possess” material is a concern for enterprises, but DPA/Police are taking a pragmatic approach.

Retention of Comms Data

- Since 2001, operators can “voluntarily” retain communications data for longer than they themselves need it (codified by EU directive 2006/24/EC, as waiver on Data Protection principles; S.28 and S.29 of DPA 1998 also provide general protection).
- Data Retention and Investigatory Powers Act 2014 puts this on a statutory footing, with S.1 notices allowing SoS to mandate retention
  - Probably mainly DHCP/Radius logs, but we don’t know
  - In principle every packet header
- NB: does NOT permit retention of content, or permit SoS to mandate retention of content.
- More retention (definitely packet headers, cf. Internet Connection Records) coming in IP 2016, but we haven’t seen the codes of practice in detail yet.

Jigsaw Attacks not Covered

- Current Information Commissioner guidance does not regard as sensitive two independent data sets which are each themselves not sensitive, but when joined are
  - eg, health records with name replaced by nonce, and a second set of records mapping name to nonce.
- Also not obvious that identifiable anonymised data (postcode + DoB is unique, for example) is covered.
- Result: headers of IP packets not under DPA, even if links mylaptop.bham.ac.uk and embarassing.website.com.

The care.data debacle

- Common problem is over-estimating impact level of data you hold (cf. companies claiming to have “IL5”, which they almost always don’t)
- However, bad things happen when you under-estimate impact level or public concern
- care.data: database of all hospital events and GP interactions, as a research and commissioning tool: not aggregated, but anonymised
- Parliamentary Evidence session was a complete car crash, and culminated with ministerial apology for misleading parliament
- Mixture of health-naive IT people and InfoSec-naive health people conspired to make fools of each other, and the project was canned.
    - Which is a shame, as the research would have been valuable. Sign up to UK.Biobank, please.
- Hammers home need to understand the data you are holding, its legal status, and the reputational risk of disclosure.

This all makes firewalls OK

- Have been arguments that firewalls might contravene DPA!
- Not valid.
- However, DPI almost certainly does: look up the debacle of Phorm.

Unsolved Problems

- Virus Scanners look at content
- Spam Filters do as well (in most cases)
- Are these interception per RIPA 2000? Are these processing per DPA 1998?
  - Confusion over this led to problems with voicemail's status and collapse of Hacking Trial investigations
- "Doormat principle": once it's on your doormat, it needs a search warrant, not an interception warrant.
  - Where is your electronic doormat?

Intercept Readiness

- Distinction between operator and enterprise much more slippery than it used to be
  - WhatsApp are a telecoms operator in every obvious way, but aren't an OLO. Not regulated by Ofcom, which means fewer obligations. *A fortiori* for Skype.
- RIPA 2000 allows installation of "black boxes" and has a fairly flexible definition of what a telecoms operator is. IPA 2016 extended this.
- Ability to provide a feed of data from a core switch might save a lot of grief, unless you have a taste for prison cells.

Intercept Readiness

- Old-school telcos maintained cell of people with DV clearance who were employees, but able to action intercept on behalf of government (list of people for whom there are active intercept warrants is classified, for obvious reasons).
- Not obvious that is the case now, and intercept may need to be done without operator knowing who is being intercepted, or with government not trusting operator to hand over take correctly.
    - In any event, it should not be possible for random operator employees to discern volume/targets.
- Almost no intercept capability in DSLAMs and other exchange-premises equipment: purely Metro/core switching.

Intercept Readiness

- Commercial status of voice is unclear, but core voice switches are **old** technology: UK is all System X (70s, manufactured 80s) and small amounts of 5ESS and AXE10 (similar age design, more modern). Anything sold in UK or US has intercept as a feature (particularly System X, also preference working and massive overload control).
  - Has anyone spoken to Telent about jobs?
- “Soft Switches” inherit feature set from older equipment (or not, which is why they often fail: 999 overload control is hard)
- So voice intercept with appropriate security and handover well-embedded.
- There might be a market for data products with similar functionality for data: at the moment it’s done by filtering ilk intercept.

Little Case Law

- Operators aren't interested in fighting The Man on behalf of their customers.
  - Except for A&A and other "boutique" operators.
- 1998: median customer young, liberal and sceptical. No major terrorist threat directed at west (in UK, "the troubles" pretty much over).
- 2018: median customer older, less liberal, more trusting, world rather more unstable
  - Snowden revelations no big deal outside Guardian readers. Agencies largely trusted.

Regulation

- UK government regime overseen by Interception of Communications Commissioner, retired High Court Judge with appropriate clearance, plus small (but now more adequate) staff
- Establishment to his fingertips, but has been fairly robust over the years
- High Court Judges not easily pushed around, retired ones even less so

Regulation

- Activity by companies unregulated, and only subject to oversight if Information Commissioner becomes involved (or if an employee or customer brings a civil action)
  - IC now issuing big fines
- Bad behaviour by employer might be cited at ET, but no evidence of it happening (unfortunately, ETs are “unreported” and don’t set precedent: nothing at an EAT yet)

Conclusions

- Enterprise: OK to look at communications data, content data also OK provided you have some loose governance. AUP protects you. Theoretical ET issue, as yet untested.
- Government: definitely not OK to look at anything without following process
- Operator: content data definitely not OK, use of communications data must be fair and proportionate (DPA).
    - You aren’t registered to process your customers’ data, so cannot without a letter of comfort from government.

Outside the UK?

- I’d love to hear other countries’ experience.