Who watches the watchmen?

Ian G Batten, former Head of Information Assurance,
Fujitsu Telecoms Europe Ltd
igb@batten.eu.org

Who am I?

- Head of Information Assurance, Telecoms Manufacturing business, specialising in access. We supply about half of the ADSL in the UK and operate one of the largest unbundled networks.
- I've run email systems since 1986, starting with cs.bham.ac.uk (uk.ac.bham.cs or ...!bham-cs, indeed) and then my current employer from 1988 to date, never as my day job.
- BSc Software Engineering, 1983 to 1986, then research associate 1986 to 1988, both at Birmingham. Now back doing a PhD.

Overview

- Who wants access to private data?
- Should they have it?
- Should we as IT professionals help?
- How do we avoid going to jail?

An E-Mail time line

- 1983: A research curiosity, only used in closed, elite communities
- 1988: An academic commonplace, in wide use by non-specialists, and business that interworks with academia.
- 1993: A computing essential, in use by everyone technical, and starting to roll into mainstream use.
- 1998: Universal in business.
- 2003: Universal amongst the middle classes
- 2008: 70% of households, >90% of economically active or those with children.
- 2013: Essentially ubiquitous, mobile and fixed

An Internet Time line

- 1983: ARPA net only available to the military and researchers, Usenet starting for the rest of us.
- 1993: NSFNet becomes the Internet, everyone can use it at a (high) price. In the UK, 64K is tens of thousand of pounds per year.
- 2003: Universal access for tens of pounds per month to at least 56K, often 500K, sometimes 2M.
- 2008: ~60% of households have >500K, home access is up to 24M, availability is >99%.
- 2013: home access at 50Mbps or 100Mbps is available in urban areas, *de facto* universal service obligation.

The World Today

- Email is universal amongst large sections of society. Most businesses operate internally with email.
- Internet access in more general terms is likewise universal, and extends into most businesses and workplaces.
- Some people want the network to be ‘safe’.
- The balance between freedom and a desire to be protected is nuanced and difficult.

Issues

- People can now communicate and move data in volumes and over distances previously impossible, and censorship and control is impossible for practical purposes.
- The legal framework is distinctly unclear, and usually spans borders.
- But new communication technologies are often subject to attempted control, born of fear of the unknown.
- Electronic surveillance is very tempting when people communicate electronically.

Consider Paper Mail

- It offers little practical security.
- However, opening every letter is impractical, and there is an extensive legal and social framework.
- There is no way to trace the true sender of a letter or parcel.
- And yet, no one worries overmuch. It's always been there.
- No-one holds the post office responsible for the content of letters and packets.

Consider the Telephone

- For many years, it provided communication that was anonymous when used, but trivial to intercept. However, mass interception was impractical.
- The public grew used to anonymity, and were surprised by the implications of CLI. PAYG has brought anonymity back. Proposals to register PAYG phones are resisted (although *de facto* it's becoming harder to buy them for cash).
- Incidental design properties became key features, unintentionally. But its familiarity meant that again no-one worried overmuch.
- BT is not held liable for what is said. Although there is starting to be pressure to control the use of the network by people who are committing crimes, BT are not considered responsible.

Now the Internet

- Movement of data that has been encrypted is easy, but encryption is rare outside e-biz.
- Interception on a mass scale is suddenly very easy. Only encryption stands in the way.
- Anonymity is easy to obtain, but unlike with post and telephony it's seen as an issue.
- Things that don't cause concern with regard to post and telephony have become “problems”.
- The legal framework is constantly evolving.

What are the fears?

- Terrorism.
- Child and other pornography.
- Political subversion.
- The chit-chat of the criminal classes.
- Almost anything that people in power don't like, or the tabloids can be convinced to worry about.

The Fear of Information

- The abdication crisis was successfully kept from the general population. In the 1930s information from overseas came through narrow channels, and only a small elite had access to it (cf. Chips Channon's "Diaries").
- The Spycatcher debacle in the 1980s showed this can no longer happen: phones, faxes and cheap transatlantic flights saw to that.
- Today, information cannot be controlled other than in repressive societies, if even then. It can only be traced and followed.

The Tensions

- Because it's easy to look at data without disturbing it, and very quickly, it's tempting to do so.
- Companies believe that all their data is **<u>their</u> data**.
- Governments have a limited enthusiasm for privacy, transparency and open communication (even the “liberal” ones).
- Citizens and employees have an expectation of privacy which is often diffuse and difficult to articulate, but is definitely there.

The Big Questions

- Under what circumstances should government look at citizens' data? Who decides?
- Under what circumstances should employers look at employees' data? Who decides?
- And under what circumstances should companies look at customers' data? Who decides?

How does this affect professionals?

- As an engineer, you may be asked to provide data for:
  - Your employer.
  - Your government.
- As a manager, you may have to set policies for your engineers.
- As a citizen, it would be nice if you cared. Informed professionals can help set policy.

What are you asked to do?

- Investigate individuals.
- Investigate groups.
- Monitor whole populations (of a country or of a business).
- Control whole populations (of a country or of a business).

The UK Legal Framework

- Data Protection Act
  - Personal data should be kept private, except for defined and permitted purposes
- Regulation of Investigatory Powers Act
  - Provides wide-ranging powers, with controls for government and employers, especially over traffic data and encryption, and may limit actions by others (cf. poor legal advice on phone hacking).
- Human Rights Act
  - Right of privacy is in conflict with RIPA.
- Sexual Offences Act 2003
  - Creates limited defence via S.46 for system administrators

Traffic Data vs Content

- Most demands for information from government are for traffic data — logs, billing records, etc.
- This requires at most a senior police officer's formal request, but is often handed over to fairly junior officials.
- Content of calls and emails requires a warrant.
- In fact, it's patterns of communication that are most often wanted.

Government access to data

- Crime Prevention
- Crime Detection
- Intelligence Gathering
- Political purposes
- “Traffic Information” pretty much on demand
- Content requires a warrant under RIPA 2000

Employer Access to Personal Data

- By personal I mean email, web access, etc.
- Many employers believe all data on their equipment, and all data accessed in their time, is theirs.
- RIPA 2000 agrees with them.
- Human Rights Act and the Halford case disagree.
- You don't want to be the test case.

Why do Employers do it?

- Fear of legal action or embarrassment.
- Fear of employees not working properly.
- IT staff with time on their hands
- HR departments with a taste for power
- Because they can!

Scenarios you may encounter

- Police serve you with a Data Protection Act S.29 notice.
  - This does not require you to comply.
  - It just allows you to voluntarily help without DPA risk
  - Get consent from senior management.
- Employer asks you to track data on employee.
  - RIPA 2000 allows you to do so, in most cases.
  - HRA and Halford Case provide limits.
  - You should get legal advice, and/or ensure that the HR department takes responsibility.

More Scenarios

- IT Manager decides to check on “legitimate” use.
  - Probably covered by RIPA.
  - Probably not HRA compliant.
  - Probably of little value to the business — what staff do with their time is a line-management issue.
  - Access to traffic data is almost certainly OK.
- You go fishing on a quiet afternoon
  - Don't do this.

Yet more scenarios

- You are asked to block access to some URLs
  - Clearly legal in the workplace
  - Unclear who is being protected, and from what
  - Frighteningly popular as a “solution” to “problems”.
  - The software is almost always aimed at conservative American parents.
- You are asked to remove a customer's website
  - Often no law involved, just a request
  - Depends on contractual terms, but usually legal
  - Someone is going to get sued for this

And yet more...

- You are served with either a search warrant or an instrument under the Regulation of Investigatory Powers Act
  - You must comply.
  - You should immediately seek legal advice, as failure to act properly may expose you to action from the owners of the data you expose.
  - This is all very murky and untested water.

Myths about Interception

- You are not liable for what your employees download, provided you have clear policies which forbid it.
- But storing it on your disks is a problem, as it may constitute possession.
- You do not need to retain data any longer than you need it for.
- There are no laws preventing the use of encryption in the UK. Perfect Forward Secrecy is legal.

Does privacy matter?

- “Those who would trade liberty for temporary security deserve neither” – Benjamin Franklin
- More to the point, it doesn't work anyway, as East Germany proves.
- “Those with nothing to hide have nothing to fear”
- But widespread telephone tapping would cause major outcry. Why is email and web access different?
- Does surveillance stop crime?