Network Monitoring & Measurement: Privacy and Legal Issues

Andrew Cormack,
Chief Security Adviser, UKERNA
A.Cormack@ukerna.ac.uk

Disclaimer

I am not a lawyer

This is not legal advice

Different laws in different countries

Talk to your own lawyers before taking action

Terminology

Active measurement

- Measurer generates own traffic and watches result
- E.g. ping, traceroute, …

Passive monitoring

- Monitor looks at headers of other people's traffic
- E.g. netflow, …

Interception

- Interceptor can see content of other people's traffic
- E.g. network sniffer …

Privacy Issues

Looking at someone else's traffic breaches their privacy
- Good practice should protect privacy as far as possible

Looking at headers seems less serious than content
- Headers are "stuff needed to get message from A to B"
  - So networks have to look at headers anyway
- But even headers can still be a serious breach of privacy
  - Suppose you find lots of packets to a cancer support site?
- Aggregating/anonymising headers reduces breach

Passive Monitoring and Interception always breach privacy

Laws exist that protect privacy

What Laws Apply? (Europe)

Active measurement

- No legal issues, provided you measure consenting targets and don't flood the network!

Passive monitoring

- Data Protection (95/46/EC) & Privacy and Electronic Communications (2002/58/EC) Directives protect people
- Confidentiality Law protects organisations

Interception

- European Convention on Human Rights (Art.8) protects humans
- Plus Data Protection/Confidentiality Law as above

Does Law Allow Privacy Breaches?

Yes, but only if they are

- Necessary, proportionate, controlled and not secret

Law balances harm if done versus harm if not done

Law recognises that some actions are needed, e.g.

- Management of billing or traffic (operations)
  - Also includes planning, capacity management, etc.
- Prevention or detection of faults & misuse
- Providing value-added services

Almost always need to tell users beforehand

- General notice, specific information, explicit consent

National Laws

Member states need to implement European law

DP Directives (headers) are detailed and prescriptive

- National laws should be similar (but are not identical)
- UK: Data Protection Act 1998 & Electronic Communications (EC Directive) Regulations 2003

ECHR Article 8 (content) has more room for variation

- National laws likely to have significant differences
- UK: Regulation of Investigatory Powers Act 2000

UK law on informing users

	Passive Monitoring (DPA 1998)	Interception (RIPA 2000)
Operation	N	N (by DPA)
Misuse	N	I or C
Value-Added service	N (user has right to opt out)	C

N: must notify users, i.e. publish the information somewhere

I: must take "all reasonable measures" to inform users

C: must obtain positive consent from ***all*** affected users

Example: checking network status

Often done by Active Measurement (ping++)

- Avoid privacy problems by measuring known targets
- Some tools measure capacity by flooding ☹

Looking at flows may be Passive Monitoring

- Aggregate data to anonymise as soon as possible
- Protect the data against disclosure/misuse

Done by network operator for operational purpose

- Remind users about it in your terms & conditions

Example: network fault finding

May include all types of measurement and monitoring

- Operator is allowed to make own network work
- If necessary and proportionate, not a problem
- General notice to users: remind them you are looking

Where possible, follow documented process

- Effective fault finding *and* effective privacy protection
- What to do when you find something unexpected?

Don't investigate other people's networks without asking

Example: investigating misuse

Logfiles are result of Passive Monitoring

- May also contain content (e.g. Subject:, URL file, …)
- So rules for interception may apply

What kind of misuse? And who is investigating?

- Technical misuse investigated by network operator
  - Part of operations: can Passive Monitor or Intercept if necessary
  - General notice to users probably sufficient
- Policy breach investigated by user organisation
  - Not part of operations: probably restricted to Passive Monitoring
  - Likely to need to inform users and make rules/punishments clear

Sharing Information with others

Must be necessary, proportionate, open, etc.

Within European Economic Area (EEA)

- Usually not a (large) problem
- Written procedures a good idea

Outside EEA

- Big problem if personal data included
- Written agreement probably essential to avoid trouble

Data relating to crimes, e.g. hacking

- Some Member States restrict this to authorised bodies
- Check whether yours requires prior authorisation

So Must Ask (and Write Down)

Are my activities necessary, proportionate, controlled, open?

- Why am I going to do this?
- Is the risk if I don't do it greater than the harm if I do?
- Can I do it in a less intrusive way?
- How long do I need to keep the data?
- How will I protect the data and the user against misuse?
- Have I informed users? Have they consented?
- What does the law require of me?

Responsible, professional activities will usually be ok

Unprofessional activities may be unlawful