



Network Performance Measurement: Privacy and Legal Issues

Andrew Cormack, UKERNA

A.Cormack@ukerna.ac.uk

Terminology

Active measurement

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

Passive monitoring

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

Interception

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



Privacy Issues

Looking at someone else's traffic breaches their privacy

Looking at headers is 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



Legal Issues (Europe)

Active measurement

- No legal issues (unless you DoS 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) applies
- Plus Data Protection/Confidentiality Law as above



Does Law Allow Privacy Breaches?

Yes, but only if they are

- Necessary, proportionate and controlled

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

- Management of billing or traffic (operations),
- Prevention or detection of misuse
- Providing value-added services
- Not clear if unanonymised "research" is allowed except as part of planning/operations

Almost always need to tell users beforehand

- General notice, specific information, explicit consent



National Laws

Member states need to implement European law

DP Directives are detailed and prescriptive

- Ought to be similar laws in all Member States
- UK: Data Protection Act 1998 & Electronic Communications (EC Directive) Regulations 2003

ECHR Article 8 has more room for variation

- Different national rules likely
- UK: Regulation of Investigatory Powers Act 2000

UK law on informing users (UK)

	Passive Monitoring (DPA 1998)	Interception (RIPA 2000)
Operation	N	N (by DPA)
Misuse	N	I or C
V-A service	N (can opt out)	C
"Research"	None, N or C	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



So Must Ask (and Write Down)

Why am I going to do this?

Is the risk if I don't do it greater than the breach 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 against misuse?

Have I informed users? Have they consented?

Some activities will be unlawful and thus prohibited