Managing Privacy in Network Operations: Learning from the Law

Andrew Cormack
Chief Regulatory Adviser, JANET(UK)
Andrew.Cormack@ja.net
Operators/CSIRTs

- Can be a serious risk to user privacy
  - Easy to get carried away and go too far
  - Or follow personal motivation
  - Or be told to do something inappropriate
How to do it right?

• Leave it to individual conscience?
  – Unlikely to be comfortable, or consistent
• Mistakes may have legal consequences
  – For you, your organisation, and the bad guys
• Better to have a document to follow
Searching for Guidance

• Laws on privacy exist
  – Often expressing clear principles

• Content:
  – European Convention on Human Rights (ECHR)

• Envelopes/Traffic:
  – European Data Protection Directives

• Content more ‘private’ than envelopes
  – So expect stricter laws/rules
  – But following the same pattern
ECHR Article 8

Right to respect for private and family life

Everyone has the right to respect for his private and family life, his home and his correspondence.
Breaching the Privacy Right

• ONLY if necessary and proportionate
  – In the interests of national security
  – To protect public safety or the economic well-being of the country
  – To prevent disorder or crime
  – To protect health or morals
  – To protect the rights and freedoms of others

• Breach must be covered by law/rules
Data Protection (95/46/EC)

- Processing of personal data must be lawful and fair to the individuals concerned;
- In particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed;
- Such purposes must be explicit and legitimate and must be determined at the time of collection of the data;
- The purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified.
Guidelines and Laws

- Guidelines say what you should do
- Laws say what you must do
  - Laws of your own country,
  + of the country where you are,
  + of the country where your company is,
  + maybe, of the country where your users are,
  + perhaps others too
- Guidelines can provide more detail or a higher standard, if you choose to adopt them
- You can’t opt out of the laws
Guidelines for CSIRTs

Whether to act (HR)
• Know what objective is
• Do no more than is necessary
• Find a reasoned, reasonable balance
  Harm if we do v. harm if we don’t

How to act (DP)
• Act (if at all) in least intrusive way
• Follow documented procedures
• Ensure powers aren’t abused
  Serious breach of trust if so
• Tell users what we will do
  And what the rules are

Your laws may demand more, or less
Ask a lawyer in your own country, not me!