# Law and regulatory issues

TkL Markus Peuhkuri

2007-04-24

## Lecture topics

- Legal issues
- Main focus on Finland (EU)
- IANAL, law is not a set of axioms
  - however, law must be understood by common people (in Finland)
  - do not try to make overly complex loophole scenarios
- After this lecture, you should
  - have some idea of laws governing information security

## Why government cares for security

- Privacy
- Important systems must available
- Resolving crimes
- Intelligence

## Short summary of Finnish governance

| | |
|---|---|
| **Acts** * are given by Parliament | laki |
| **Decrees** * are given by Ministries | asetus |
| **Regulations** * are given by officials to whom right is given by an Act or a Decree | määräys |
| **Special enactment** * dictates ruling different from general act* in a specific situation | erityislaki<br>yleislaki |

## (Data) security governance in Finland

- Ministry of Transport and Communications* — Liikenne- ja viestintäministeriö
  - FICORA (Finnish Communications Regulatory Authority*) — Viestintävirasto
- Ministry of Justice* — Oikeusministeriö
  - Office of the Data Protection Ombudsman* — Tietosuojavaltuutettu toimisto
- Ministry of Trade and Industry* — Kauppa- ja teollisuusministeriö
  - Consumer Agency* (Consumer Ombudsman*) — Kuluttajavirasto
  - National Emergency Supply Agency* — Huoltovarmuuskeskus
- Ministry of the Interior* — Sisäministeriö
  - Police

# Privacy

- Governed by multiple laws
  - Personal Data Act* (523/1999) — Henkilötietolaki
  - Act on the Protection of Privacy in Electronic Communication* (516/2004) — Sähköisen viestinnän tietosuojalaki
  - Communications Market Act* (393/2003) — Viestintämarkkinala
  - Act on the Protection of Privacy in Working Life* (759/2004) — Laki yksityisyyden suojasta työelämässä
- A message that is not intended to public, is confidential regardless of medium
  - unintended recipient may not disclose even existence of message
  - one may return to sender

# Personal Data Act

- General act on processing of personal data
- Furthermore 650 acts gives detailed instructions
- Key terms

| | | |
|---|---|---|
| **personal data** | * information on a private individual related to an identifiable person or family | henkilötieto |
| **processing of personal data** | * is any action done on personal data | henkilötietojen käsittely |
| **personal data file** | * is a storage where personal data can be retrieved easily and at reasonable cost | henkilörekisteri |
| **controller** | * who determine use of data file | rekisterinpitäjä |
| **data subject** | * is subject of personal data | rekisteröity |

- Duty of care
  - good processing practice
  - safeguards for private information
- Use of personal data must have a defined purpose that is a real one and not one dictated by technology
- Data may not be used for a purpose that is incompatibe with original purpose
  - historical, scientific and statistical purposes are not incompatible

# SVTSL

- Act on the Protection of Privacy in Electronic Communication* (516/2004) — sähköisen viestinnän tietosuojalaki
- Replaces Act on the Protection of Privacy and Data Security in Telecommunications 22.4.1999/565
- Implements EC Directive on Privacy and Electronic Communications* (2002/58/EC) — sähköisen viestinnän tietosuojadirektiivi
- Covers
  - public communication networks
  - networks attached to public networks
  - secrecy and privacy in internal (restricted) networks

## Definitions in SVTSL

**message** * is a phone call, e-mail message, SMS message, voice message or any comparable message sent in — viesti

**communications network** * is any system using electromagnetic means to transport message — viestintäverkko

**public communications network** * is a network available to set of users without any prior restriction — julkinen vv

**telecommunications operator** network- or service provider

**network service** provision of a communications network by a telecommunications operator for providing

**communications service** means the transmission, distribution or provision of messages

**value added service** using identification data or location

**identification data** associated to subscriber or user

**location data** indicates the geographic location

## Definitions in SVTSL

**subscriber** a legal person or a natural person

**corporate or association subscriber**

**user** a natural person

**information security** administrative and technical measures to protect data

**processing** means collecting, saving, organising, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions.

## Act on the Protection of Privacy

- Sets demand on
  - network and service providers
  - value-add service providers
  - corporate subscribers
  - users of network
- Handling of *identification data*
  - any data that records existence or details of a message
- Corporate subscriber
  - organisation, that has users using services provided
  - may also be the other party in communications
  - usually a bystander
  - ultimately responsible even if services outsourced

## Who has a right to handle identification data

- To realise services
  - even automatic handling for relaying is handling
- To implement data security
  - firewalls, virus scanners
  - must not infer with legal communication
- For charging
  - in most cases, no reason to reveal B-number
    $\Rightarrow$ aggregate information sufficient
- To improve technical implementation
  - only aggregate or anonymous information
- To resolve technical problems
- To resolve misuse
  - *not* to follow where a employee visits or what messages sends (unless identified as virus)
  - misuse must have some direct costs
- Communicating parities
- If permission by one of communicating parties

## How to handle identification data

- Only when needed
- Only as much as needed
- Only those whose duties it belongs to
- Handing information over only to those that have right
- Service provider must have audit trail for two years
- Professional discretion must be maintained

## Information security and privacy

- Corporate subscriber *must* take case of identification data security
- Threats on information security
  - may take actions to protect system security
  - remove malicious payload
  - refuse from accepting messages
- Must not exaggerate actions
  - no limit freedom of speech or privacy
  - must stop as soon as there is no immediate need
  - filtering should be done without accessing message content

## Act on the Protection of Privacy in Working Life

- A special act for Personal Data Act and Act on the Protection of Privacy in Electronic Communication
- Rules for
  - handling employee personal data
  - tests for employees
  - technical survellance
  - opening emails
- Strict rules for what is allowed
  - uneven situation between employer and employee: “this is ok, isn’t it — or do you want to start looking for a new job”
- Technical supervising and data networks use
  - employees must be informed in cooperation procedures

## When it is allowed to open employee email

- Employer must provide methods to avoid it
  - automatic vacation replies indicating period of absence and contact for another person taking care of tasks
  - directing emails to another address or person
- Employer may search for messages if
  - employer manages task individually
  - is evident that such message is sent
  - employee cannot perform one’s tasks
  - employees consistent cannot be obtained withing time
  - or if employee is permanenty incapaeble

## How to open employee email

- With help of system administrator employer may search for messages using message
  - sender
  - receipient
  - title
  - date that must be close to absence period
- Search and/or opening is documented
  - two persons
  - report delivered to employee as soon as possible
  - opened message must be saved
- Use of role addresses and ticketing systems helps a lot
- Better to have private email address

## Communications Market Act

Public communications networks and communications services and the communications networks and communications services connected to them shall be planned, built and maintained in such a manner that:

1. the technical quality of telecommunications is of a high standard;
2. the networks and services withstand normal, foreseeable climatic, mechanical, electromagnetic and other external interference;
3. they function as reliably as possible even in the exceptional circumstances referred to in the Emergency Powers Act and in disruptive situations under normal circumstances;
4. the protection of privacy, information security and other rights of users and other persons are not endangered;
5. the health and assets of users or other persons are not put at risk;
6. the networks and services do not cause unreasonable electromagnetic or other interference;
7. they function together and can, if necessary, be connected to another communications network;
8. terminal equipment meeting the requirements of the Radio Act can, if necessary, be connected to them;
9. they are, if necessary, compatible with a television receiver that meets the requirements of this Act;
10. their debiting is reliable and accurate;
11. access to emergency services is secured as reliably as possible even in the event of network disruptions;
12. a telecommunications operator is also otherwise able to meet the obligations it has or those imposed under this Act.

## Information security on Communications provider (FICORA 47B 2004M)

- Administrative security* — Hallinnollinen tietoturvallisuus
  - organisational security (ISO 17799)
  - documentation
    - high-level principles
    - detailed information for day-to-day operation
  - liabilities and resources
  - frequent evaluation and updating
  - security auditing
  - outsourcing
- Personal security* — Henkilöstöturvallisu
  - background checks
  - avoiding dangerous positions: ones where there is no another person supervising other or where one can cover her tracks.
- Communication security* — Tietoliikenneturvall
  - information of communication may not be disclosed to third parties
  - must have user identification / authentication / non-repudiation systems
  - able to limit or filter traffic

## FICORA 47B 2004M

- Equipment and software security* — Laitteisto- ja ohjelmisto-turvallisuus
  - security threats must be controlled
  - no unnecessary services
  - backup systems and backup data
- Documentation security* — Tietoaineistoturvall
  - information classification
  - rights based on tasks, access control
- Usage security* — Käyttöturvallisuus
  - controlled risks
  - rights only for those who need those
  - bookkeeping who has right to where
  - no unauthorised use
  - security violations must be identified

## Responsibilities in outsourcing

- Provider ultimately responsible
- What are roles:
  - provider ⇔ outsourced
  - when a contractor becomes a provider?

## Importance classification Ficora 27 E/2005 M*

Yleisen viestintäverkon tärkeysluokittelu

- It is not economical to protect all systems similarly
- Classification based on impact
- Important system* — Tärkeä järjestelmä
  - serious risks of unauthorised access
  - difficult to replace
  - disruption has an effect on 1/3 of numbering area (based on number of subscribers or by area)
  - disruption has an effect on more than 10000 customer of public broadcasting network
- Very important system* — Erittäin tärkeä jäjrestelmä
  - high importance to service continuity or during state of emergency
  - relays significant proportion of important community traffic
  - disruption covers whole numbering area
  - disruption covers all public broadcasting network
- Physical security, backup power

## Examples of important systems

- Important exchange in numbering area
- Important exchange in long-distance network
- Control room of mobile network
- SMS exchange
- Core network router
- Authentication server
- Name server
- Server hotel
- Broadcasting station for more than 10000 subscriber
- System serving more than 100 voice subscriber: POTS, VoIP, mobile radio voice channels, PBX connections

## Examples of very important systems

- Most important exchanges of long-distance network
- Network management servers for very important systems
- Mobile network exchange
- Mobile network and IN databases
- Root name servers
- Internet exchanges
- National DVB multiplex management system
- System serving more than 500 voice subscriber: POTS, VoIP, mobile radio voice channels, PBX connections

## Decrees on email

- Ficora 11/2004M
- Prohibiting open relays
  - must disconnect if one found
- Consumer SMTP traffic through provider system
  - inbound, outbound
  - provider may provide open access
    - must inform customer
    - must be able to react quickly
- Malicious email traffic
  - filtering of traffic
  - ability for emergency filtering
  - must disconnect host sending malicious traffic
- Must monitor email system performance
  - delay, system load
  - breaks by type
  - information about filtering
  - number of disconnected subscriber connections
- Must have standard mailboxes: security, abuse, noc, postmaster

## Authorised wiretapping

- Prohibited in Finland before 1st June 1995[1]
- Wiretapping* Telekuuntelu
  - listening or recording of message
  - for serious crimes; it is also allowed on some lesser crimes in which it is difficult to get evidence without wiretapping
- Remote surveillance* Televalvonta
  - identification information from messages, not content
  - location info
  - for crimes that maximum penalty is at least four years
  - crimes done though communication network
  - also information about all mobile devices around some place at certain time
- Telecommunications operator must provide capacity for both
- Requires court order; remote surveillance allowed by officer's order in urgent situation. Must notify court within 24 hours.

## State of emergency

- How to protect communications in crisis
  - logical and physical protection
- Information warfare
  - disrupting normal communications
  - spreading false information
- Additional communications
  - priority calls
  - emergency switching: non-priority calls are blocked

## Reporting responsibility

- Telecommunications provider must report to FICORA
  - security violations
    - break-ins to provider systems
    - sensitive information disclosure
    - degenerated performance because of attack (DOS, SPAM)
    - malicious software in provider system
    - social engineering
    - unauthorised wiretapping equipment
  - security threats
    - serious break-in attempts
    - anomalous traffic
    - new security problems in provider systems
  - serious system malfunction or disruption
    - breaks longer than one hour affecting many subscribers
    - very important system malfunction more than 30 minutes
- Customers must be informed
  - customer education
  - information about implemented protection measures like email filtering

[1] Pakkokeinolaki

## How about international issues

- Which law should be enforced
  - server location
  - user location
  - service provider location
- Standpoint by country (note: extremely glib)

  **user privacy** Northern Europe
  **government rights** Mediterranean Europe, Asia
  **corporate rights** USA

  - who owns your personal details: you or collector
- War on terror adds law enforcement powers

## Summary

- Laws and regulatory actions needed
- Several aspects of security must be covered
- Important to classify
  - connections
  - equipment
  - documents
  - data sources
  - people

  to maintain security