

# Law and regulatory issues

Markus Peuhkuri

2005-04-26

## 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 make overly complex loophole scenarios

## Why government cares for security

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

## Short summary of Finnish governance

**Acts** are given by Parliament

**Decrees** are given by Ministries

**Regulations** are given by officials to whom right is given by Act or Decree

## (Data) security governance in Finland

- Ministry of Transport and Communications<sup>1</sup>
  - FICORA (Finnish Communications Regulatory Authority<sup>2</sup>)
- Ministry of Justice Oikeusministeriö
  - Office of the Data Protection Ombudsman<sup>3</sup>
- Ministry of Trade and Industry<sup>4</sup>
  - Consumer Agency<sup>5</sup> (Consumer Ombudsman<sup>6</sup>)
  - National Emergency Supply Agency<sup>7</sup>
- Ministry of the Interior<sup>8</sup>
  - Police

---

<sup>1</sup>Liikenne- ja viestintäministeriö

<sup>2</sup>Viestintävirasto

<sup>3</sup>Tietosuojavaltuutetun toimisto

<sup>4</sup>Kauppa- ja teollisuusministeriö

<sup>5</sup>Kuluttajavirasto

<sup>6</sup>Kuluttaja-asiamies

<sup>7</sup>Huoltovarmuuskeskus

<sup>8</sup>Sisäministeriö

# Privacy

- Governed by multiple laws
  - Act on the Protection of Privacy in Electronic Communication<sup>9</sup> (516/2004)
  - Personal Data Act<sup>10</sup> (523/1999)
  - Communications Market Act<sup>11</sup> (393/2003)
- 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

## Act on the Protection of Privacy in Electronic Communication<sup>12</sup> (516/2004)

- Replaces Act on the Protection of Privacy and Data Security in Telecommunications 22.4.1999/565
- Implements EC Directive on Privacy and Electronic Communications<sup>13</sup> (2002/58/EC)
- Definitions

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

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

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

**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** shows the geographic location

**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.

- Covers
  - public communication networks
  - networks attached to public networks
  - secrecy and privacy in internal (restricted) networks

---

<sup>9</sup>Sähköisen viestinnän tietosuojalaki

<sup>10</sup>Henkilötietolaki

<sup>11</sup>Viestintämarkkinalaki

<sup>12</sup>sähköisen viestinnän tietosuojalaki

<sup>13</sup>sähköisen viestinnän tietosuojadirektiivi

## 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 outsourced

## Who has 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  
⇒ 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)
- 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 care of identification data security
- Threats on information security
  - may take actions to protect system security
  - remove malicious payload
  - deny accepting message
- 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

## 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 (FI-CORA 47B 2004M)

- Administrative security<sup>14</sup>
  - organisational security (ISO 17799)
  - documentation
    - \* high-level principles

---

<sup>14</sup>Hallinnollinen tietoturvallisuus

- \* detailed information for day-to-day operation
- liabilities and resources
- frequent evaluation and updating
- security auditing
- outsourcing
- Personal security<sup>15</sup>
  - background checks
  - avoiding dangerous positions: ones where there is no another person supervising other or where one can cover her tracks.
- Communication security<sup>16</sup>
  - information of communication may not be disclosed to third parties
  - must have user identification / authentication / non-repudiation systems
  - able to limit or filter traffic
- Equipment and software security<sup>17</sup>
  - security threats must be controlled
  - no unnecessary services
  - backup systems and backup data
- Documentation security<sup>18</sup>
  - information classification
  - rights based on tasks, access control
- Usage security<sup>19</sup>
  - 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 contractor becomes provider?

---

<sup>15</sup>Henkilöstöturvallisuus

<sup>16</sup>Tietoliikenneturvallisuus

<sup>17</sup>Laitteisto- ja ohjelmistoturvallisuus

<sup>18</sup>Tietoaineistoturvallisuus

<sup>19</sup>Käyttöturvallisuus

## Importance classification Ficora 27 E/2005 M<sup>20</sup>

- It is not economical to protect all systems similarly
- Classification based on impact
- Important system<sup>21</sup>
  - 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<sup>22</sup>
  - 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

---

<sup>20</sup>Yleisen viestintäverkon tärkeysluokittelu

<sup>21</sup>Tärkeä järjestelmä

<sup>22</sup>Erittäin tärkeä järjestelmä

## 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<sup>23</sup>
- Wiretapping<sup>24</sup>
  - 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<sup>25</sup>
  - identification information from messages, not content
  - location info
  - for crimes that maximum penalty is at least four years
  - crimes done through 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.

---

<sup>23</sup>Pakkokeinolaki

<sup>24</sup>Telekuuntelu

<sup>25</sup>Televalvonta

## 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

## 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