



# The EU Telecommunications Privacy Directive

**Security and Privacy**  
**VSE Prag, 9 - 13.6.2008**

Institute for Information Processing and  
Microprocessor Technology (FIM)  
Johannes Kepler University Linz, Austria

E-Mail: [sonntag@fim.uni-linz.ac.at](mailto:sonntag@fim.uni-linz.ac.at)  
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



- Applicability
- Security
- Confidentiality
- Anonymisation requirements
- Itemised billing
- Location data
- Subscriber directories
- Spam
- Practical Aspects
  - Cookies
  - Logging



- Directive from 2002 replaces a directive from 1997
  - Important change since then: Internet and mobile phones
    - » Did exist then, but became a mainstream mass-market
- Main aspects are therefore
  - Traffic data
    - » How long may it be stored? Use for other purposes?
  - Location data
    - » When/how can it be used for what services?
  - Calling/connected line identification
    - » How/when to suppress it; overrides for special purposes
  - Subscriber directories
    - » The right not to be included; special search functions
  - Unsolicited communication
    - » Combating spam...



## Applicable area

- Processing of personal data
  - Only of natural person!
- relating to provision of publicly available el. comm. services
  - Conveyance of signals
    - » Excluded are content providers; only the transmission itself
  - Closed networks are not affected, only public providers
  - Communication services must be electronically, i.e. excludes the old (analogue) telephony system
  - Normally provided for remuneration
    - » Private WLANs with public access are included!
- in public communication networks in the EU
- Excluded are (similar to the privacy directive)
  - Public security, defence, state security, criminal law
- Opening clause for call line identification/forwarding
  - Technically impossible or disproportionate economic effort



- Broadcasting services are excluded: There are no individual endpoints of the (completely unidirectional) communication
  - "Finite number of parties"
    - » Conference calls are included!
- But if there are identifiable subscribers or recipients, the communication is subject to this directive!
  - Webradios will fall into this category: They can identify the individual persons receiving their streams
    - » Note: This doesn't require perfect identification (name, address, ...); the identification by a specific IP address is sufficient!
  - This also includes video-on-demand
    - » Obviously: Individual billing



- Traffic data

- Data processed for the conveyance of an communication or for the billing

- » Includes IP addresses, routing data, "Received" headers, ...

- » Includes also subscriber information ("billing")!

- Static IP address, physical address, login time/duration etc.

- Content data: "Inner data", i.e. speech, mail text, ...

- Location data

- Any data processed in an el. comm. network indicating the geographic position of the terminal equipment

- » Typical example: Cell ID of mobile phones

- » Also: IP address - provides hints to a geographical location (e.g. ISP in Germany)!

- E.g. Lati-/Longti-/Altitude, direction of travel, level of accuracy, cell identification, time the location information was recorded



- Appropriate technical and organisational measures required to safeguard the security of its services
  - If necessary together with other providers, e.g. upstream ISP
- Required level is determined by:
  - State of the art
  - Cost of the implementation
  - Appropriate to the risk
- Conclusion: Do the same as most of the others do!
- In case of particular risks of breach of security
  - Provider must inform subscribers
    - » E.g. important systems have been found to be vulnerable
  - Risk outside scope of measures to be taken by provider
    - inform about remedies and likely costs
      - » If its too costly to repair (see above!) → Users should do it



# Confidentiality

- Confidentiality must be protected by prohibiting
  - All kinds of interception or surveillance (listening, tapping, ...)
  - Concerning the communication itself and the traffic data
    - » The latter need not be personal data!
- Still possible to allow:
  - Storage of comm. by user with consent of the users
    - » Recording a phone call after telling the other person
    - » In the course of lawful business practice to provide evidence
    - » Only when legally authorised!
      - Illegal in some countries → Need not be legalized or prohibited
  - Wiretapping ordered by courts, ...
  - Technical storage necessary for the transmission
    - » I.e. no duplicates, immediately deleted after hand-off
  - Full consent by user
  - Strictly necessary for service explicitly requested by the user



# Anonymisation requirements

- Traffic data must be anonymized when it is no longer needed for the transmission
  - E.g. dynamic IP addresses → Delete when connection closed
- But several exceptions exist:
  - Subscriber billing and interconnection payments
    - » Note: The latter is "invisible" to the end-user!
    - » So: Dynamic IP → Deletion only with "flat rate", but not "fair use"!
    - » Information on types of traffic data and its duration required
  - With the users consent (withdrawable any time) for marketing el. comm. Services or the provision of value added services
    - » Information on types of traffic data/duration required in advance
    - » Differs from privacy-consent: Not specific!
  - Generally:
    - » Restriction to data necessary for the purposes above
    - » Handled only by a certain subset of employees (cust. enquiries, fraud detection, ...)



# Itemised billing and privacy

- Subscribers have the right to non-itemized billing
  - I.e., on request you must receive an anonymized bill
    - » No individual calls, only a total value to be paid
  - There is no right to an itemized bill in the directive!
    - » Most countries do have such a right!
- National provisions must be made to reconcile itemised bills with the right to privacy of calling and called users
  - Example: Alternative privacy enhancement methods
    - » Typically removing the last N digits of the number
    - » Calling cards/credit card payments (anonymous phones)



# Processing location data

- Regulated is only location data **other** than **traffic data**!
  - This is data not necessary for the provision of the service
    - » Example: The IP address is location and traffic data → Excluded
- Processing only allowed anonymously
- Or with consent of the subscriber to extend and duration necessary for providing a value added service
  - Information on type of location data, purpose duration, transmission to third parties; only what is necessary
  - Withdrawal of consent possible at any time
    - » Note: Privacy → Exception for fulfilling a contract → Here not!
  - Continuous, simple & free possibility of temporarily refusing processing of such data for each connection/communication
- Restricted to persons acting under authority of provider
  - Or the third party providing the value added service



# Directories of subscribers

- Information free of charge before inclusion
  - Purpose and any further electronic search possibilities
    - » Example: Searching for a name by telephone number
    - » This practically excludes online lists → Only search applications
      - With a limited number of responses/query length (NOT: "a\*", "b\*",...)
- Users may decide which data is to be included
  - Limited by the purpose of the directory
    - » Purpose: Determined by the provider of the directory
- Opting out must be possible free of charge
  - As well as verification of, correcting, or withdrawing data
- Member states may require consent of the user, if the search capabilities exceed "details by name"
- Only applies to natural persons
  - Legitimate interests of other subscribers must be sufficiently protected by national legislation

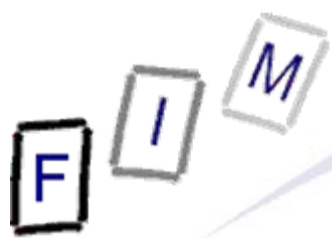


# Directories of subscribers

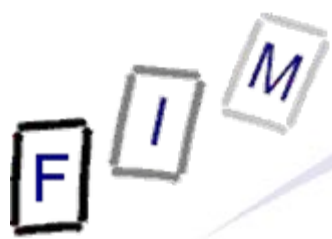
- Potential problem: WHOIS!
- Is this a "directory of subscribers"?
  - » Unclear!
  - It looks very similar
  - It is not mainly about "communication services"
    - » They are not subscribers to the network
    - » Such a directory would be a list of domain names sorted by the name of their owner
- Basic idea:
  - Not: "I have a name, how can I contact this person?"
  - Rather: "I have contact information, who owns this?"
- Note: WHOIS is a privacy problem anyway!
  - Therefore "anonymisation" exists in the form of companies acting as trustees
  - But: Land registers are usually not anonymous either...



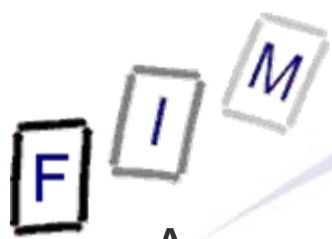
- Automated calling systems, fax machines and el. mail
  - Prior consent required for direct marketing
  - Electronic mail includes SMS, MMS, ...
    - » Any text, voice, sound, or image message which can be stored in the recipients equipment until collected by him
- For all other communication methods, the member states can decide between opt-in and opt-out
  - But it must always be possible free of charge!
- These apply to natural persons only
  - Other persons (i.e. companies) must be sufficiently protected
    - » Example: Austria had opt-out for them, but later changed it to opt-in, similar to natural persons
- Always prohibited is sending E-Mail for direct marketing
  - Disguising or concealing the identity of the sender
  - Without valid address for opting-out



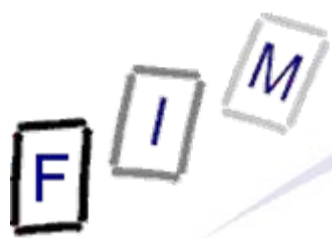
- Exception, but **only for electronic mail**:
    - Contact details obtained in the context of a sale
      - » Need not be an actual sale; also negotiations sufficient
        - Mere inquiries are insufficient!
    - Only this person (natural or legal)
      - » Selling of the contact details is forbidden
    - For direct marketing of its own similar products/services
      - » No advertising foreign products
      - » No advertising completely unrelated products
    - Opportunity to object free of charge and easily
      - » On collection of the contact details
      - » In each and every message
- ⇒ "Follow-up/Cross-selling" marketing is allowed



- What is a "cookie"?
  - Small (max. 4 kB) text file with data
  - Content (incl. Exemplary information):
    - » Name: "session-id"
    - » Value: "028-3057779-9388524"
    - » Domain: ".amazon.de"
    - » Website-Path: "/"
    - » Expiry date: 8.11.2006, 23:59:05
    - » Secure (https): \*
- Problem: The values can be any information
  - A part of it might be the IP address
    - » Or the users login name, local customer number, ...
  - Or it might be a random number uniquely assigned on visiting the web site and deleted afterwards



- Are cookies personal data?
  - If yes, full privacy legislation would apply (→ consent, ...)!
    - » But they are very useful and typically not dangerous at all
      - Regarding privacy; not necessarily from security (session hijacking!)
- Classification of cookies:
  - Usually they are personal data for sites with registration
    - » After login, the connection to a certain user is known
      - Need not be a fully identified person (name, ...)
      - Typically have a long lifetime (avoid re-login)
  - Mere session-cookies for websites are usually anonymous
    - » Just a random number and nobody (except the data subject itself) could align it to a certain person
      - Typically deleted when browser shuts down
      - Tied to an IP address → might be personal data
- Guidelines for cookies (but only in recitals!):
  - Information of users that they are used, purpose, content
  - Opportunity to refuse



- Access to a site may be made conditional on its acceptance
  - Conclusion: Consent necessary together with login
    - » "Remember me on this computer", ...
- "Dangerous" versions of cookies
  - Third-party cookies
    - » Site x.at sets a cookie for y.at: x.at cannot read it, only y.at
      - Actually a kind of data transfer (which?) from x.at to y.at!
      - Option "Accept cookies for originating site only"
  - Mixed content
    - » Banner from another server can set their own cookie
      - This is not a third-party cookie, as it comes from the same server as the advertisement content (usually image)!
      - Data transfer still possible through the image URL



- What to do (ideally):
  - No cookie on homepage
  - Information page on what a cookies, what it is used for, what information is stored in it (and when, if login exists), and when it will be transmitted (=on every request to this site)
  - Webform with checkbox "I allow setting a cookie"
- What to do (practically):
  - Anonymous (session) cookie on homepage
    - » Stored only until browser is closed
  - Information on privacy page: Content see above
  - Login page associates anonymous cookie internally with the customer record (no personal data in cookie)
  - Option on login for a permanent cookies (checkbox)



- Logs occur very often and may contain a lot of personal data:
  - Weblogs: Server/Proxy
  - Mail-log, traffic(IP)-log, DHCP-log, security-logs, ...
- Are these "personal data"?
  - Depends on the content!
  - Usually they are, as they are made on firewalls, i.e. on the company perimeter, and the company knows its employees
    - » IP/ E-Mail addresses can be associated with single persons
  - Not necessarily personal data: Webserver logs (ext. visitors)
    - » See cookies: Login? → Personal data
- But: Some technical monitoring is necessary!
  - To what degree/details? "Legitimate interests"?
    - » Often anonymous or at least reduced data logging is sufficient
  - No "reusing" this data, e.g. for verifying working time!



# Logging: Examples

- Webserver log:
  - 192.168.1.1 - - [03/Aug/2005:09:05:00 +0200] "GET / HTTP/1.1" 200 7277
- Mailserver log:
  - Nov 2 10:48:22 firewall sendmail[29980]: kA29mlo6029980: from=<someone@xyz.de>, size=225534, class=0, nrcpts=1, msgid=<4549CCCA02000008000BD3B2@oesnwgwn03.xyz.lan>, proto=ESMTP, daemon=MTA, relay=mail.xyz.de [192.168.1.1]
  - Nov 2 10:48:37 firewall mimedefang.pl[11148]: MDLOG,kA29mlo6029980,mail\_in,,,<someone@xyz.de>,<recipient@msv.at>,**Antw: AW: Brief**
  - Nov 2 10:32:40 firewall pop3[29412]: login: [192.168.1.1] *someUserName authMethod* User logged in



- The directive regulates individual elements of privacy in the telecommunications area
  - Not all of it relates to the Internet!
  - But with VoIP, this might change as well
- Important aspects are
  - Spam: Opt-in for fax and E-Mail
  - Deletion of traffic data
  - Cookies (only regulated indirectly)
- The main and important regulations are still to be found in the main privacy directive!

F I M

# Questions?

Thank you for your attention!