



Mag. iur. Dr. techn. Michael Sonntag

The EU Telecommunications Privacy Directive

Security and Privacy
VSE Prag, 7 - 11.6.2010

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

E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



Agenda

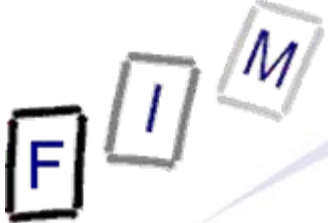
- Applicability
- Security
- Confidentiality
- Anonymisation requirements
- Itemised billing
- Location data
- Subscriber directories
- Spam
- Practical Aspects
 - Cookies
 - Logging



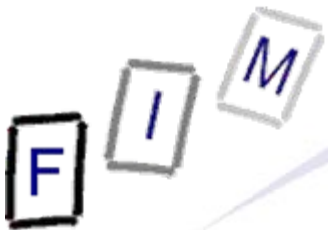
- Directive from 2002 replaces a directive from 1997
 - Important change since then: Internet and mobile phones
 - » Did exist then, but became a mainstream mass-market
- Amended 25.11.2009 by directive 2009/136/EC
- Main aspects are therefore
 - Traffic data
 - » How long may it be stored? Use for other 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...



- 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 or service 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

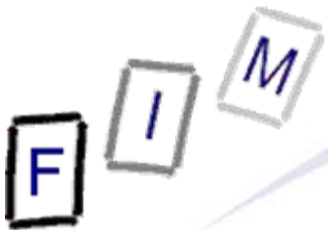


Confidentiality

- 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 communication 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



- Privacy must be protected according to normal privacy law
 - Rep.: Only authorized person can access personal data for legally allowed processing
 - Rep.: Protection of personal data from accidental or unlawful destruction/modification/storage/processing/disclosure/transfer
 - Enforcement of a security concept for processing pers. Data
 - » You must create one and you must enforce it
 - Content is not specified: This directive + privacy directive + ...!
- National authorities can inspect measures taken for privacy and can issue recommendations



Data Breach Notification

- In case of personal data loss/destruction/.... you now **must**
 - Immediate notification of the supervisory authority (SA)
 - If it is to be expected that the users are affected in their private sphere, these users must also be notified immediately
 - » This is not necessary if it is proven to the supervisory authority that sufficient technical precautions had been taken and that these were used on the data in question. Such measures must be an encryption of the data for all unauthorized persons.
 - Problem: What if it was an insider? Then the encryption is useless! Is then still no information of the users required?
 - » Supervisory authority can always request such a notification
- A notification must include
 - Type of infraction of privacy: Loss/disclosure/...
 - Contact point for more information
 - Possible actions to limit detrimental consequences
 - Only to SA: Implications and suggested/implemented actions



Data Breach Notification

- Technical rules for when/how and procedure of notification can be issued by the commission
 - If not present, the supervisory authority can issue rules
 - » When a notification of users must take place
 - » Format and procedure of notification
 - SA can verify compliance enforce it through sanctions
- Every processor of personal data must keep a list of such problems
 - Including circumstance of the problem
 - Including consequences of the problem
 - Including measures taken to reduce consequences/prevent additional problems
 - Must be sufficient to allow the SA to verify compliance
 - No other data may be stored in there
 - » E.g. the names of the persons whose data was lost



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 of 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, ...)



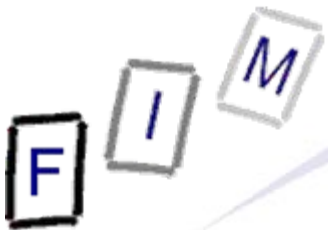
Itemised billing and privacy

- 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!
 - » But 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)



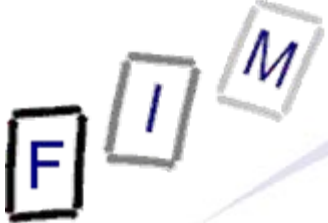
Processing location data

- 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 extent 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: Sending E-Mail for direct marketing when
 - disguising or concealing the identity of the sender,
 - without valid address for opting-out,
 - in contravention to information requirements from EC directive
 - » Must be clearly identifiable as commercial
 - » Person who instructed the send them must be clearly identifiable
 - » If price reductions/free add-ons/gifts etc. are allowed in a country these must be clearly identifiable as such and conditions for obtaining them must be easily accessible, clear & unambiguous
 - » If lotteries and similar things are allowed in a country they must be clearly identifiable and the rules must be easily accessible, clear & unambiguous
 - or where the recipient should visit a website which is in contravention to the information requirements listed above
- The last two are new from the amendment!

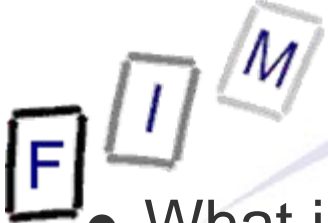


- Exception, but **only for electronic mail**:
 - Contact details obtained in the context of a sale
 - » Need not be an actual sale; also negotiations sufficient
 - Mere inquiries are insufficient!
 - Only this person (natural or legal)
 - » Selling of the contact details is forbidden
 - For direct marketing 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

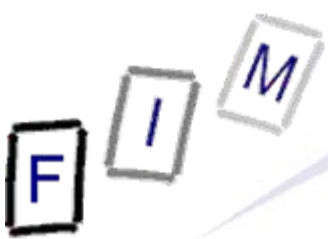


Spam: Enforcement

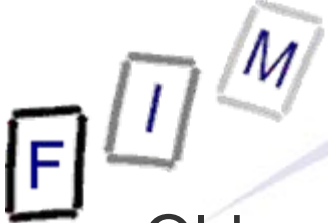
- Prosecution through courts must be possible for natural or legal persons adversely affected through infringements
 - If they have a legitimate interest in the cessation or prohibition of such infringements
 - Regardless of any administrative penalties
- This explicitly includes the service providers!
 - Which means, not only the recipients but also the ISP can bring legal actions against spammers
- Reverse: Member states **may** introduce punishments for service providers contributing to spam through negligence
 - Active battling against spam would then be a legal requirement for them!



- 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
- Note: Legal rules apply to other technologies equally!
 - Example: Flash cookies, DOM storage, ...



- 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 temporarily personal data and later anonymous
 - » Just a random number and only the ISP (later nobody) can align it to a certain person
 - Typically deleted when browser shuts down



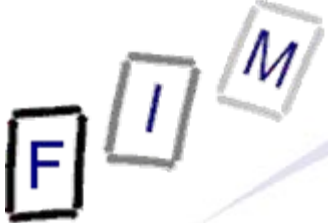
- Old guidelines for cookies (but only in recitals!):
 - Information of users that they are used, purpose, content
 - Opportunity to refuse
- New guidelines for cookies (but only in recitals!):
 - Clear and unambiguous information for actions, which might lead to their storage
 - Method of information and the opportunity to decline should be as user-friendly as possible
 - Exclusion only if strictly necessary for requested service
 - » Does not apply to cookies!
 - If technically possible, the consent of the user can consist in the configuration options of the browser/similar software
 - » At best implied consent; never explicit!
- Legal rule: Instead of “opportunity to refuse” a requirement of “clear and comprehensive information” + “consent”



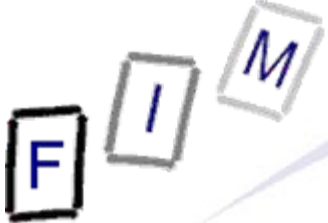
- Access to a site may be made conditional on its acceptance
 - Conclusion: Consent necessary together with login
 - » "Remember me on this computer", ...
- Whether session cookies are still allowed is currently unclear
 - Some say no as there is no consent
 - » Browser configuration might be enough...
- "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" (typ. active today)
 - 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 cookie is, 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; probably legally allowed):
 - 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)
 - » Otherwise only a session cookie



- 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 amendment introduced required enforcement
 - Previously: Each state used some kind (or no) enforcement
- However, the EU has no competence for punishment
 - Therefore the typical requirement only:
 - Effective, proportionate and dissuasive
 - Even possible if breach has been rectified: For full duration!
- Supervisory authority must be empowered and possess enough resources (!) to supervise and enforce the directive
 - Current practice: Very little personnel and money!



- 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!