



Mag. iur. Dr. techn. Michael Sonntag

Data Retention

Datenschutzrecht

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>



- What is data retention and why is it necessary?
- The EU directive on data retention
 - What is retained and what not
 - Who is obliged
 - Who may access the data for what reasons
 - Safeguards: Security & privacy
 - Overview on national implementations: Austria, Germany
- Discussion of the directive: Aim, pros, cons
- Options for technical implementation of the directive
 - IP addresses
 - E-Mail communication
 - VoIP communication
- Alternatives



What is "data retention"?

- Data retention (DR) is the keeping of data for further use, which would have otherwise been deleted
 - Here, we are talking about "telecommunications DR"
 - Even more specific, about data retention of Internet comm.
- Subject of DR discussed here:
 - IP addresses
 - Communication acts within the Internet
 - » TCP connections, E-Mails, web sites visited, chat sessions etc.
- DR is nothing new and has existed for many decades
 - Pursuant to court orders telephones were fitted with tape recorders to identify the numbers dialled and all sound
- Problematic and currently hotly discussed is DR, which is independent of any suspicion:

Mandatory retention of all communication of all customers



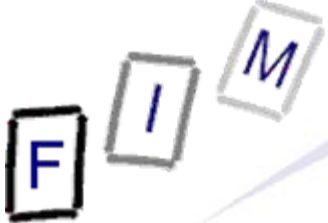
Why is it needed?

- Basic idea: Going back in time!
 - DR allows investigating communication after it took place
 - » Typical "normal" DR only works from a point on ("realtime")
- Commercial companies employ data retention to learn about their customers
 - Examples: Google, Amazon
 - Typical usage: Personalization, invoicing, legal obligations, ...
- DR as discussed here:
 - Judicial proceedings (criminal and civil)
 - » File sharing, libel, hacking, espionage, ...
 - Police investigations
 - » Confirming suspicions, identifying accomplices, ...
 - Combating terrorism
 - » Uncovering terror networks, identifying accomplices



Data retention vs. computer forensics

- Often a forensic examination only results in IP addresses
 - Examples: Tracing the origin of an E-Mail, intrusions
- As these occurred in the past, data from that point in time is required to identify the computer involved
 - Note: Dynamic IP addresses are (sometimes) allocated frequently to different persons, so they change over time!
 - Note: Typically not the computer but only the Internet connection can be identified, much less the actual user!
- If the retention occurs on the device under investigation (=log files), this provides additional information
- Another aspect of CF, e.g. after intrusions, is checking whether any kind of "malicious DR" took place
 - Keyloggers, snapshots, screenshots etc.



The EU directive

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

- Enacted: 15.3.2006; to be transposed: 15.9.2007
 - Internet part may be postponed up to 15.3.2009
 - » Many countries did this, including Austria!
- Basic idea: Combat terrorism and "serious crimes"
 - ... investigation, detection and prosecution of serious crime, as defined by each member state ...
- Problems: Proceedings whether it was enacted correctly
 - Directive would "disappear" if procedure/basis was incorrect
 - This would **not** affect the national laws!
 - Decision: Was correct → No changes
- Background: London/Madrid bombings



What is to be retained?

- The following data should be collected:
 - » To identify both natural persons and legal entities
 - Trace and identify the source of a communication
 - » Calling telephone number, name and address of user, UserID
 - Trace and identify the destination of a communication
 - » Number dialled, final destination number (call forwarding, call transfers, ...), name and address, UserID
 - Identify the date, time, and duration of a communication
 - » Date & time of:
 - Start and end of communication of fixed network&mobile telephony
 - Log-in and log-off of the Internet access, IP address, UserID
 - Log-in and log-off of Internet E-Mail services
 - Log-in and log-off of Internet telephony services
 - Identify the type of communication
 - » Telephone service used (voice call, voicemail, fax, S/M/EMS, ...)
 - » Internet E-Mail and telephony: the Internet service used



What is to be retained?

- The following data should be collected:
 - Identify the communication equipment
 - » Fixed network telephony: Calling and called telephone numbers
 - » Mobile network telephony: Calling and called telephone numbers, IMSI and IMEI of caller and called
 - » Prepaid anon. services: Date, time and CellID of initial activation
 - » Internet access/E-Mail/telephony: Calling telephone number (modem dial-up), DSL/other endpoint of the communication
 - Identify the location of mobile communication equipment
 - » CellID of the start of the communication
 - » Geographic location of cells by CellID
- Period of retention: Minimum 6 month
 - But see e.g. Poland: Initially planned 15 years for storage, but finally settled on two years!



What is **not** to be retained?

- Unconnected calls
 - Calls, where the destination number does not exist
 - When the recipient doesn't answer this must be retained for the full time, but **only** if the information is **already stored**
 - » But there is no obligation to store it!
- Any content data (expressly forbidden)
 - This might be difficult in practice...
 - » Example: Mails to order@sadomaso.com, help@drugabuse.com



- Providers of publicly available electronic communication services or of public communications networks
 - Only within the EU (i.e. within each member state)
- "Publicly available electronic communication services" =
 - Wholly/mainly conveyance of signals
 - available to general public
 - normally provided for remuneration
- "Public communications network" =
 - Electronic communications network
 - used wholly or mainly for the provision of
 - publicly available electronic communications services (↑)
 - » Explanation of the German law-draft: This excludes company-internal networks, PBX, E-Mail servers of universities providing services exclusively to students and faculty, and the communication infrastructure in the medical area



- Internet E-Mail & telephony: Obligations may apply only to data from the providers own services
 - » Stated in the (non-binding!) reasons
 - I.e., providers will probably not be required to log all traffic to port 25 on other servers, but only to their own server!
 - » Using the provider's SMTP server → DR
 - » Using the provider's IMAP/POP server → DR
 - » Sending an E-Mail directly to a server outside the EU would not be logged at all!
 - See e.g. the German law-draft!
 - » Using an IMAP/POP/webmail server outside the EU → No DR
 - » Only the IP address can be associated to the user
 - » Everything else would be **MOST** complex and expensive!
 - No monitoring port 25
 - No investigation of web traffic whether it is a webmail page



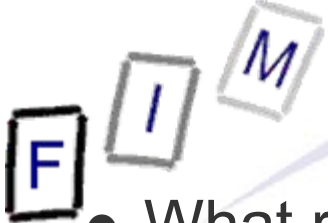
"Normally provided for remuneration"?

- Must be some kind of commercial undertaking
- Private commercial undertaking
 - "Private" use is excluded
 - » Does this apply to Fon/Freifunk?
 - German decision: Fon is unfair competition → So it's commercial
- Remuneration need not stem from the customer
 - Commercial free TV: Paid for by the advertisers
- Problem: Must the remuneration be the “main source” of income, i.e. is the service only an “add-on”?
 - Some say: Internet Cafes are not required to do DR, as the main income is from selling coffee, not internet access
 - » Would also apply to e.g. Hotels, requiring payment for WLAN
 - My opinion: This doesn't matter!
 - » Internet Cafes: You don't go there to **just** drink a coffee...



"Normally provided for remuneration"?

- Unclear: Whether "normally" depends on this service provider or the service in general
 - Always free at this provider, but such a service must be paid at all other providers?
 - » Public WLAN hotspots – You have to pay for at hotels, ISPs, ...?
 - This type of service is free, but "better" ones cost money?
 - » Typical example of webmail: Basic version is free, but spam filtering, more space, etc. costs money!
 - Locally or globally (→ universities!)?



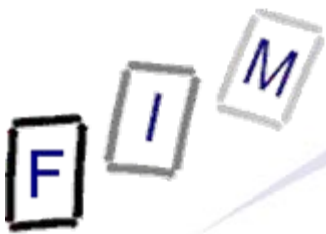
"Public service"?

- What restrictions are necessary to be "non-public"?
- One approach: In effect the access depends "only" on the **payment** for the service
 - Universities would be excluded; in Austria students must have the "Matura" to be accepted (but then **must** be!)
 - Companies would be excluded, as employees will only be hired if the company needs them and finds the individual "ok"
 - Problem: ISPs!
 - » They accept customers only in the area they can actually supply their service (→ characteristic of the provider!)
 - » But this could be seen as a "local" public service
 - » Also, this depends on the characteristic of the service itself
- Counterargument: Set up company for commercially providing service only to a clearly defined subset of citizens!
 - E.g. some car insurances are available solely to women!
 - Internet access only with computer driving license !?!



Example: Universities

- Position of the Austrian ministry of education:
Universities are not public → No DR (would be too costly!)
 - "Club of all persons allowed to study" → Only members can obtain Internet access from an associated company
 - » Is this still "public?"
 - Universities with access restrictions?
 - » E.g., universities of applied sciences (Fachhochschulen)
- But: "normally provided for remuneration"
 - Austria studies are "free", as the study costs are only nominal
 - This does not apply to fully-paid courses
 - » Which also exist at many universities!
 - Does this affect the university not at all, only these studies, or is the whole university then suddenly "for remuneration"?
 - Consider also private universities!



Who may access the data?

- Who may access the data?
 - Only "competent national authorities"
 - » Will be defined by each member state!
 - Only in specific cases
 - » Not to be used for general computerized searches
 - In accordance with national law
- National laws for procedures and conditions must
 - adhere to the necessity and proportionality principle
 - conform to European law, national law, and especially the European convention on human rights (ECHR)
- What is missing?
 - What may be done with the data afterwards?
 - » Indefinite usage/storage?
 - » Or do the "normal" privacy rules apply? ← Presumably!



Reasons/causes for access

- The main issue (and discussion!) is, for which offences the privacy of the user might be "broken" through accessing the retained data
 - Probably nobody has a problem with terrorism
 - But also possible for kids sharing a single music file
 - » And what about those offering 100 songs in a P2P network?
- Additional: Safeguards through procedure
 - Can anyone/the police/a judge request such information?
 - What amount of "proof" is required?
- Directive: "serious crime"
 - Considerations of the directive:
 - » "serious matters such as organised crime and terrorism"
 - Austrian proposal: "serious crime"
 - More details later!



Privacy safeguards through providers

- The data collected must be treated according to the normal privacy laws/directive unless changed for DR
- Additional explicit requirement:
 - Access may only be possible to personnel specifically authorized to do so
 - » Additional encryption or authorization (log-in), ... necessary
 - Data must be destroyed and the end of the retention period
 - » Unless it was accessed and preserved
 - E.g. for ongoing proceedings
 - » This is technically not that easy to realize!
 - Is this to be done daily/weekly/monthly/yearly?
 - How to exclude this specific data from deletion?
 - » Unclear is the collision with other rules/permissions:
What if this data is necessary for other legal purposes and might be stored, used, ... according to privacy laws?



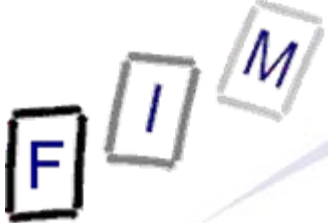
Security safeguards through providers

- Data must be of the same quality, and subject to the same protection, as the data on the network
 - Quality: States that we may not "reduce" the data in any way
 - Protection: If we don't secure the data on the IP network at all, do we have to protect the stored IP addresses at all?
 - » But see next requirement!
- Data must be subject to appropriate technical and organisational measures to protect it against
 - » accidental or unlawful destruction,
 - » accidental loss or alteration, or
 - » unauthorized or unlawful storage, processing, access or disclosure.
- This is technically not that easy and requires probably extensive precautions (to be further detailed in laws)

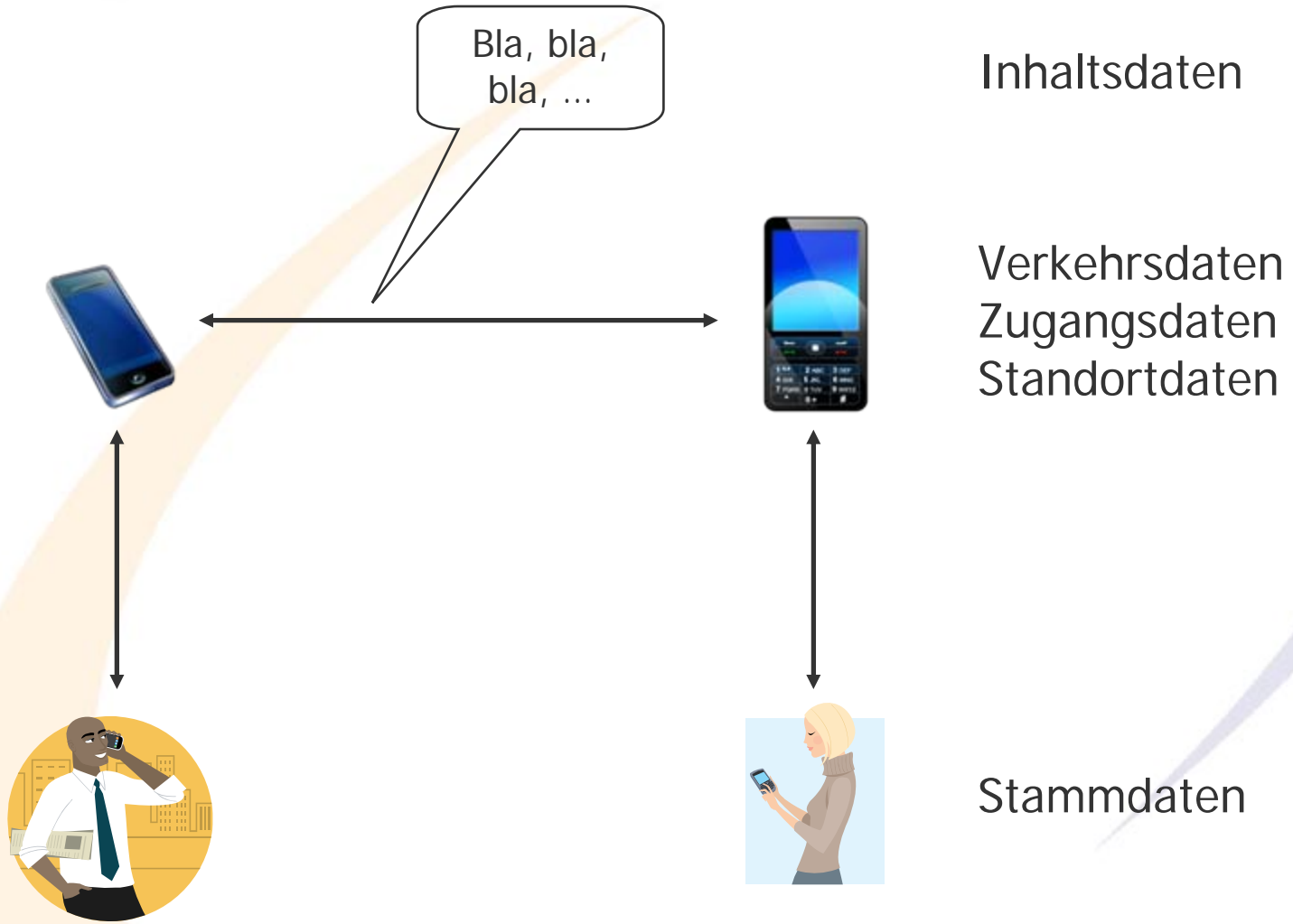


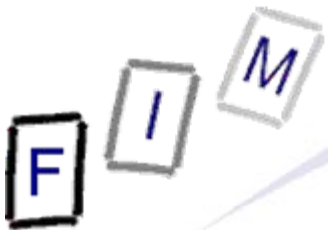
Data classification in Austria

- Stammdaten: Required for the contract
 - Name, ac. title, address, participant number (e.g. telephone number), type and content of contract, creditworthiness
 - » Includes IP address only if it is assigned within the contract
- Verkehrsdaten: Data processed for transmitting a message in a communication network or for invoicing it
 - E.g. calling&called telephone number
- Zugangsdaten: Those “Verkehrsdaten” created when connecting to a public communication network, and which are necessary for assigning the network address to a communication at a certain point in time
 - E.g. IP address assigned by the ISP; “a static IP” in contract
- Inhaltsdaten: Content of a communication
 - E.g. text of E-Mails, spoken word of telephone calls
- Vorratsdaten: Data retained **solely** because of data retention



Data classification in Austria



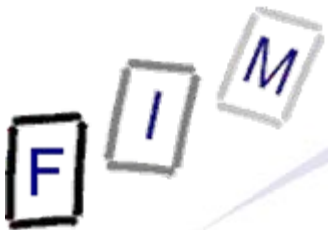


Data retention in Austria: “Standard” disclosure

- Disclosure of Stammdaten (exkl. creditworthiness)
 - On suspicion of an administrative transgression performed by employing a public communication network
 - » Only if it doesn't require processing of Stammdaten
 - » Example: Sending Spam
 - Request (in writing, with reasons) of competent courts, public prosecutors, police or security authorities
 - » Only if it doesn't require processing of Stamm-/Vorratsdaten
 - » For solving “specific crimes”
 - Details in other laws, especially the StPO
- Disclosure of Verkehrsdaten for any crime according to StPO to any of the official authorities allowed there
 - This might be **ANY** data, but only as long as it is present!
 - » No retention!
 - Requires a court order

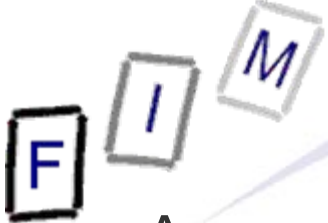


- Every service provider must have all necessary equipment ready for monitoring messages and disclosure of stored or retained data
 - An adequate compensation will be determined by regulation
- For every monitoring or disclosure an adequate compensation will be paid
 - Determined by regulation
 - Must take into account any interest by the company (???) and the potential danger to be countered by the act
 - » Terrorist acts → No compensation
 - » Filesharing → Compensation



Data retention in Austria: Technical details

- Any disclosure has to be transmitted
 - Encrypted and in CSV format
 - By E-Mail (It seems no fax disclosure is allowed anymore!)
 - Details will be set by regulation
- Storage requirements:
 - Disclosure must be possible immediately (during office times)
 - Data must be stored so that it can be identified as “data-retention data”, i.e. separate storage or explicit marking
 - It must be protected from accidental or unlawful destruction or disclosure



Data retention in Austria: Logging

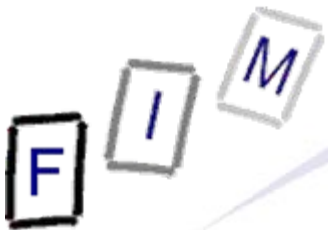
- Any access to retained data and any disclosure of it must be logged in detail with following information:
 - Reference to court order
 - Date of request and date+time of disclosure
 - Number of records disclosed
 - Duration of storage of disclosed data at time of disclosure
 - Name and address of the user, whose data was disclosed
 - Unique ID of the person which performed the disclosure
 - May **not** contain the disclosed data itself!
- Complete log must be sent yearly to the ministry of justice
 - Also on request; + on request to data protection commission
 - The log of disclosure is sent yearly to the ministry
- Problem:: The ministry receives a list of names and addresses of all persons which were “suspect” in the last year for free!



Data retention in Austria

- Duration: 6 month after termination of communication
 - End of ISP connection (might be days/weeks!)
- Deletion: Immediately, at most one month after expiry
 - Useful for backups!
 - No disclosure after expiry, even if not yet deleted
- Only for discovery and prosecution of serious crimes
 - Problem: **No definition at all what is “serious”!**
- Disclosure of retained data:
 - Requires a court order
 - Must be based on a law explicitly referencing § 102a TKG
 - “Push”, not “pull”: No access by the police, only by the ISP
- Excluded from the obligation of data retention are:
 - Small or very small companies
 - » <50 employees, <= € 10 Mio turnover, <= € 10 Mio total assets
 - » Must be determined by notification from the ministry

Attention: This is according to the (new) draft! This law has not yet been enacted and might be changed yet!



Data retention in Austria: What to retain (1)

- Telephony, including VoIP

- » VoIP = Packet based and IP protocol based

- » Must be a public telephony service: Requires to be part of a national or international numbering plan

- This probably excludes Skype and all other “private” services!

- Calling and called participant ID (e.g. telephone number)

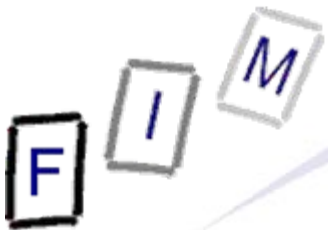
- » And names and addresses of the resp. subscribers

- Which are not necessarily the participants of the communication!

- Redirection → Where the called is routed to

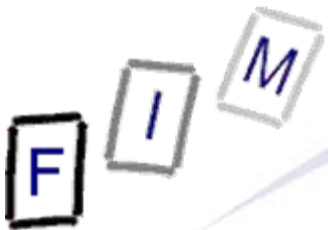
- Date and time of start and duration of communication

- Type of communication (voice, fax, SMS, ...)



Data retention in Austria: What to retain (2)

- Internet access providers
 - Name, address, ID and public IP address at any time
 - » Including the timezone, i.e. exact time!
 - Date & time of assignment/revocation of public IP addresses
 - Calling number/line ID of the internet access
- E-Mail service providers
 - E-Mail address for every customer
 - Name and address for every person assigned an E-Mail address at every point in time
 - E-Mail address and public IP address of sender and E-Mail address of recipient of every E-Mail sent
 - E-Mail address of sender and IP address of last communication step of every E-Mail received into a mail folder
 - Date, time, ID and public IP address of every login and logout to E-Mail service



Data retention in Austria: What to retain (3)

- Only data that is processed must be retained
 - Example: Address of recipient of VoIP call will almost always be unknown (unlike their telephone number!)
 - Freemail providers: No name/address
 - » No requirement to obtain them!
- E-Mail: Communication using SMTP protocol
 - Includes Webmail, if it employs SMTP
 - Stored are the envelope addresses, not the one from the headers (=content!)
 - Data retention for spam:
 - » If stored in a mail folder (e.g. “Spam”) or marked as such, data must be retained
 - » If it is rejected or deleted, data need not be retained



Data retention in Germany

- Length of draft: 193 pages, including explanations!
 - But includes other surveillance measures (DR: ≈19 pages)
- Retention period: 6 month
 - Must be stored within the EU
 - Deletion within one month after the 6 month period elapsed
- On call-transfers **every step** must be logged
- Data may be accessed only by certain institutions
 - Must be enabled for each area within the law
 - » Example: § 100g StPO references §113a TKG (=DR)
 - May only happen on single cases
 - » No "general" access, e.g. all data from a certain area
- If the telecommunication service is not provided directly, the provider must ensure that someone else retains the data
 - But this is to be interpreted extensively; e.g. call forwarding



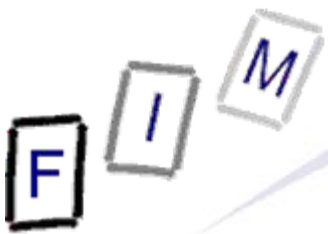
Data retention in Germany

- Data may be used for:
 - All criminal proceedings
 - » Must be explicitly provided for in law
 - Included: All crimes committed through telecommunication, serious crimes which are "also in the specific instance serious"
 - This includes all copyright infractions in the Internet ("through telecommunication")!
 - » Note: Filesharing in Germany is now usually handled like this:
 - Media company starts criminal proceedings
 - Public attorney identifies the person
 - » Newer decisions: This is not done any more → No identification anymore!
 - Public attorney drops the criminal proceedings because of little guilt
 - Media company inspects the files
 - Media company starts private proceedings
 - To prevent significant dangers for public security
 - Constitutional protection of country and states, secret service, and military secret service

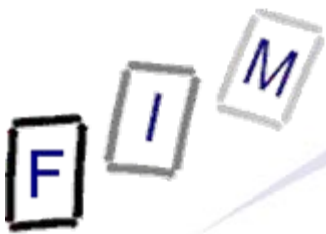


Data retention in Germany

- Anonymisation services must log all the anonymisations!
 - Law: Who changes some data must log **when** it was changed and **what** was changed to **what**
 - All anonymisation services within Germany are practically "abolished"
 - » Please note: There is a law requiring telephony providers to offer anonymous services if possible (not very strictly enforced!)
- Only data which is created or processed must be retained
 - I.e., mere transmission is not affected!
 - This means e.g. for E-Mail: Only source and destination must store the addresses/IDs/...
- Data stored **only** because of DR may not be used for anything else
 - Example: No analysis for marketing purposes!

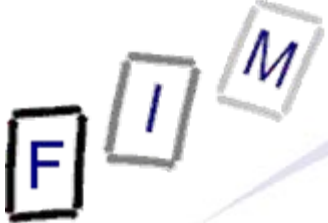


- Sweden: Infringement proceedings by the commission
 - Results (C 185/09):
 - » Sweden Lost
 - » Have to pay costs
 - » No fine
 - Comment of the minister of justice:
 - » No final conclusion reached by the public in Sweden yet, so in spite of proceedings there will be no draft law for the moment
- Romania: Law was declared illegal by constitutional court
 - VfGH 8.10.2009 Nr. 1.258
 - Contradicts telecommunication secrecy, exceptions in criminal process become the rule, removal of “innocent until proven”, data retention is excessive



What are the aims of the directive

- "Prevention, investigation, detection, and prosecution of criminal offences"
 - "Prevention" is mentioned only at the beginning
- Making sure that the anonymity in the Internet is not used to create a lawless area in effect
 - That laws **do** apply is clear nowadays
 - But currently they cannot be enforced in many cases, as the perpetrators are completely anonymous
 - » Only IP address known → "untraceable" to a single person
 - » Shipping to a physical address is also no sure identification
 - Similar to license plates on cars!
- Help in identifying the "network"/the criminal **after the fact**
 - If known in advance → current wiretapping, search etc. possibilities are already sufficient!



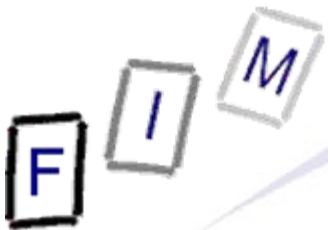
Arguments for the directive

- Recent terror attacks could be traced back to the terrorists or some accomplices through their mobile phone calls
 - But this was only possible, because this data was available!
 - » And with pre-paid phones, flat-rates, etc. this is less likely
 - Other targets are organized crime, phishing, fraud, child pornography/misuse, etc.
- While e.g. P2P filesharing by (a single!) student is not really a "serious crime", it is still illegal
 - If no tracing is possible, copyright would essentially be abolished in the Internet!
- Some countries already do have DR
 - Different models in various countries are problematic for transnational providers (especially mobile phones)

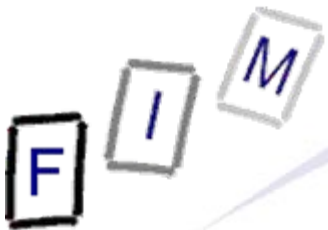


Past regulations: The Convention on Cybercrime

- An international conventions to combat cybercrime
 - Several years old (23.11.2001)
 - But in many countries not yet transposed to law
- This international convention included e.g. provisions:
 - "Quick-freeze" (Art. 16): Expeditious preservation of specified computer data, including traffic data!
 - » Preservation and maintenance for up to 90 days to allow for disclosure (e.g. to go through an judicial approval process)
 - Partial disclosure: To enable tracing the traffic to other providers to order a quick-freeze there
 - Secret real-time collection of traffic data
 - Secret interception of content data

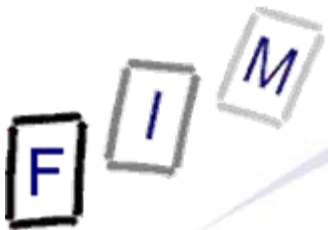


- It is very easy to avoid the data retention
 - Use pre-paid mobile phones, EU-external webmail/servers, encryption, Internet cafes, anonymisation services, ...
 - No serious criminal is likely to be caught, unless he is very careless or makes outrageous errors
 - » Might even increase the use of such services!
 - So whether it can actually reach its aims is very doubtful!
 - Therefore unsuitable as deterrent
- Storing mobile phone locations allows interesting possibilities
 - E.g. in divorce proceedings, but also as alibis
 - » This has in general little to do with serious crimes!
 - However: Presence of phone and even communication does not necessarily mean, that the **owner** was really there,...



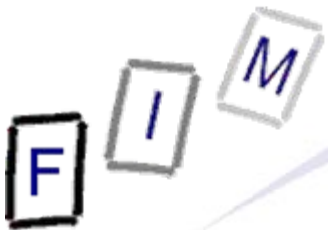
Problems of the directive (2)

- Communication analysis is possible
 - If a person repeatedly calls a psychiatrist during his office hours, this hints at an illness, i.e. sensitive data!
 - Analysis of who talks with whom is not really restricted
 - » There is no general access, yes, but still ...
 - But if a single person is known, then a network can be traced from this person on to all others
 - » This is the intention: Combating terrorism
 - » But when data exists, it can be used for other things as well!
 - Example Germany: Access for secret service!
- Unification doesn't really take place:
 - Every country can have:
 - » Different duration
 - » Different access procedures (and different entitled institutions)
 - » Different crimes (unimportant for the providers)



Problems of the directive (3)

- If you are a private person and offer a public service (which is normally offered for remuneration), DR applies
 - Example: Public WLAN hotspot → DR might be necessary
 - » This might include the obligation to identify all users!
 - » Therefore probably a problem for local public hotspots too!
 - Depends on "remuneration" → This provider or generally?
 - This also applies to E-Mail, but not to webhosting, chat, discussion groups, NetNews, ..
- Not only criminals are monitored, but everyone
 - See George Orwell: 1984!
 - Everyone is a suspect per definition
 - » And then might have to prove his/her innocence!
- If data exists, it will be used
 - The catalogue of crimes will continuously be expanded
 - » Public outrage → "Don't let them get away with it!"

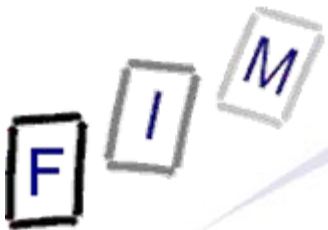


- Data is perhaps not always stored very securely
 - Not in the interest of the provider!
 - Hacking of the server or unauthorized access would lead to enormous personal information!
- In the end, all the customers will have to pay for it
 - » Some estimates: 10-15 % price increase, end of business for small providers and some webmail providers
 - Large ones might move outside the EU
 - The companies will not "swallow" this from their profits
 - Even when paid for by the state → Taxes!
- Might be against the constitution
 - Freedom of communication, privacy, ...
- A more pressing problem seems to be accessing existing foreign data, which is extremely slow or impossible



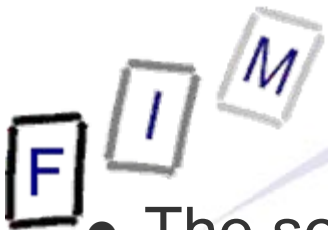
Study by the German BKA (15.11.2005)

- Study by the German Federal Policy: The solving ratio of crimes would at most be increased through DR by 0,006 %!
 - 381 (=0,006%) cases could not (?) be solved because of missing communication data in several years
 - » Two of them were from organized crime/terrorism
 - » 36% were fraud and computer fraud
 - » Not all of them might have been solved with data!
 - They just could not investigate further as no data was available
- Currently the ratio of cases solved is in telecommunications higher, and in internet fraud and software piracy very much higher than the average ratio
- Note: This study must be seen as suspect!
 - No mention what cases (should) have been reported!
 - » Or whether it was obligatory to answer



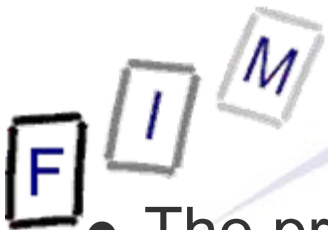
Technical implementation: IP address

- An ISP must store whenever a customer is connected to the Internet, i.e. dials in, powers his router, ...
 - Trivial with static IP addresses; these are stored anyway
 - Dynamic IP addresses: DR must take place in the future
 - » Currently: Typically already in place for accounting
 - No accounting allowed (privacy!) for customers with fully unlimited data transfer (amount and time; "fair use" does require it!)
- Technically not that hard to implement, but the storage, backup, access-restrictions, logging, etc. will require new software and regular maintenance



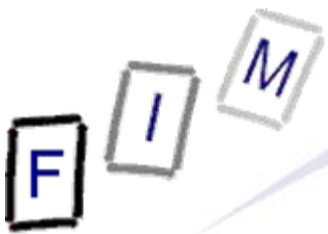
Technical implementation: E-Mail communication

- The source must store all the data
 - Example: An ISP providing an SMTP server as a proxy must store who sent an E-Mail at what time to which recipient
 - » Users send them directly without an SMTP server: No DR!
- The destination must store all the data
 - Example: An ISP receiving an E-Mail for a customer must store from whom and to whom it was sent
 - » Sending to a host under end-user control: No DR!
- The access/receipt must be logged
 - Example: When a user accesses his E-Mail by POP or IMAP, or logs in to a webmail service the ISP must log this access
 - Note: Regular checking (e.g. all 5 min.) is common → Huge log!
 - » If the service is outside the EU: No DR!
- Implementation requires server modifications
 - Logging currently possible, but not necessarily a single line/in a DB; may contain other data, e.g. the subject, IDs, ...



Technical implementation: VoIP communication

- The provider of the telephony service must store who called whom at what time
 - For example Skype must store each and every connection
 - » See SkypeOut for "remuneration"
 - But is Skype an "internet telephony service"?
 - » Skype-IDs and IP addresses
 - If Skype is located outside of the EU:
 - » If no service is offered into the EU, there is no DR obligation
 - If some users employ it "unofficially" there might still be no DR
 - » Problem: Skype cannot easily locate its users
 - What about US customers travelling within the EU?
 - Not accepting any connection from an IP address within the EU?
 - » Just "drop" EU then? Skype probably not, but smaller ones ...
- Many such services are for free in large areas
 - This data is probably currently not stored at all!
 - Only the parts to be paid for!



- Secret online surveillance
 - Would yield even more information
 - But mostly only usable "forward"
 - » Only stored mails can be investigated, but not deleted ones
 - These might be recoverable by computer forensic, but this is probably too complicated to add to online surveillance software!
- Audio-/Video surveillance
 - When monitoring the room with the computer, much information, e.g. internet telephony, can be gathered as well
 - » E-Mails are probably rather difficult to monitor
 - Usable only forward
 - Modifications of the data by the investigator impossible!
- Quick-freeze
 - Usable only forward



- Some measure of DR is probably necessary
 - To avoid the Internet becoming completely anonymous
 - » I.e. retaining solely the IP address for some time
- Logging individual communication acts is not necessary
 - E-Mail, location of mobile phones, telephone calls
 - Reasons:
 - » Too easy to subvert
 - » Not worth the effort: Very limited results
 - » Amassing data which will only be used extremely rarely
 - Or completely automatic, which is even more frightening!
- Data retention as presented here will come
 - Or, in countries other than Austria, has already arrived!

F I M

Questions?

Thank you for your attention!

See also:

<http://www.akvorrat.at/>