

Convention on Cybercrime

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>



- Why the need?
- Current state of the treaty
- Offences against data and systems itself
- Computer- / content-related offences
- Copyright-related offences
- Sanctions
- Jurisdiction
- Collection & interception of data
- International cooperation
- Reservations



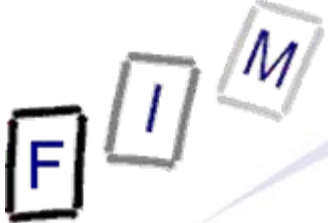
Why the need?

- The problem of jurisdiction in the Internet
 - Who is responsible for a trial?
 - How to get hold of the accused person(s) / evidence?
 - » Internationality!
 - » Digital evidence is soon lost: Logs are kept only for short times
 - See also: Data retention; Here: Quick freeze
- Computer use is often a special case
 - “Deceiving” a computer is legally impossible
 - » Austria: Fraud is only possible against humans
 - Additional crime "computer fraud"
 - Data value itself low, but expensive consequences possible
 - Evidence is easily lost
 - » Or forged: How to prove that a bit was different previously?
 - See computer forensics!
 - Computer crimes are often hard to detect
 - » The crime itself, not its consequences; example: Phishing

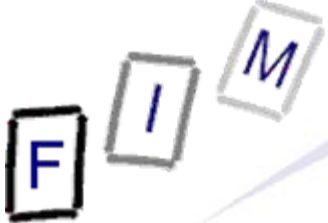


Why the need?

- Crimes can be committed over long distances
 - Many countries can be "involved"
 - » The country where the criminal was acting
 - » The country where the damage was done
 - » The country where the server employed was standing
 - » The country where the defrauded person is living
 - » ...
 - International harmonization is needed
- Some detrimental behavior is currently not illegal
 - Killing a person is known and illegal
 - » But what about "hurting" or "killing" a computer?
 - DoS, DDoS, Ping of death, ...



- “Theft” of time
 - Hacking into a computer (or extending an existing access) to use computational power and CPU-time
 - Time/service cannot be stolen
 - At most indemnification possible
- Computer “fraud”
 - A computer cannot be deceived → No fraud
 - At most indemnification possible
- DeCSS: Decrypting DVDs to view legally owned disks on a legally owned computer and operating system (Linux)?
 - Reverse engineering / publication / ... allowed?
 - What about copyright?



Current state of the treaty

- Treaty number 185 of the European Council
- Signed by 46 countries
 - Most countries of the Council of Europe
 - Plus: Canada, Japan, South Africa, United States, Mexico, ...
 - » Entry into force only for the USA, all others have not ratified yet!
- Ratified by 29 countries
 - » Excluding: Austria, Czech Republic, ...
 - Entry into force: 1.7.2004
 - » Opening for signature: 23.11.2001 → 2,5 years!
 - » Or later, for those who have ratified it since
- Many Countries added some reservations
 - Not the full treaty applies to them!
 - Territorial: Excluding Feroe Islands & Greenland
 - Content: Not Art. 9 par 2 lit b; "conduct results in serious harms as determined by applicable US federal law", ...



- Reservations to the convention are enumerated:
Only those explicitly provided for are possible
 - See the individual descriptions!
- Reservations are a common element of conventions to get many countries to agree (total consensus often impossible)
 - But still require a smallest common base
 - Other reason: Different legal systems and traditions
- Only possible at signature or ratification
 - Later on only withdrawals of reservations are possible
 - Convention urges to withdraw, but sets no time-limit
 - Periodical inquiry, whether withdrawal is possible
 - » To put some pressure for more uniform application



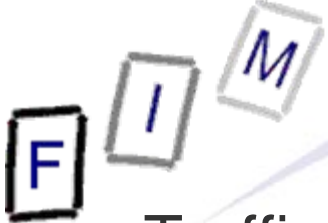
Amendments, Denunciation, Federal clause

- Amendments
 - Only possible if every single party agrees ⇒ Rare!
 - Often additional conventions are made, which change/enhance an existing one
 - » Some of the members of the first may be parties to this, but not all need to be parties
 - » Not party to the first → Cannot be party to the second alone
- Denouncement
 - At any time possible by simple notification
 - About three months time till no more binding
- Federal clause
 - Reservation possible, that the implementation will be split
 - » Must be done according to a countries constitution
 - » Only for areas of substantive/procedural law and jurisdiction



General definitions

- Computer system
 - Device or interconnected or related devices (=Hardware)
 - At least one automatically processes data
 - » (=without direct human intervention)
 - » I.e., not all elements must be computers
 - Includes power supply, printers, ...
 - Pursuant to a program
 - » =Software; set of instructions
 - Not required: Changeability! Embedded systems with hardcoded program are computer systems as well
- Computer data
 - Any representation of facts, information or concepts
 - » Includes programs, i.e. all kind of data
 - In a form suitable for processing in a computer
 - » Electronic or other; can be directly fed into a computer
 - Concept of a program on paper is not computer data!



General definitions

- Traffic data: Any computer data
 - relating to a communication by means of a computer system
 - » Endpoint information: Telephone number, E-Mail/IP address, ...
 - or generated by a computer system that formed a part in the chain of communication
 - » Control data: E-Mail "Received" headers, MAC addresses, ...
 - Indicating the communications
 - » Origin: Who sent it
 - » Destination: Who should receive it
 - » Route: What way did it take
 - » Time/Date/Duration: When and how long did it take
 - » Size: How large was it
 - » Type of underlying service: What was it (phone, E-Mail, chat, ...)
 - For tracing source/sink of communication
- Not included: The content itself!
 - I.e. the voice itself, the E-Mail body, the chat messages, ...!



Definitions: Criminal offence

- “Criminal offence” as defined by the convention (Art 2-11)
 - Convention knows civil, criminal, and administrative liability
 - » See Art. 12 para 3 (corporate liability)!
 - Offences must be “criminal” however, so administrative punishment is not enough!
 - Punishment: Effective, proportionate and dissuasive
 - » Must include deprivation of liberty
 - This is usually the domain of criminal law in most countries, at least if longer sentences are involved
 - » Corporate liability (Art 12): Must include monetary sanctions
- All offences are punishable **only** when committed **intentionally**, never by negligence!
 - Sometimes additional intentional elements required (e.g. Art 8)
 - Countries **may** be stricter and also punish negligence!



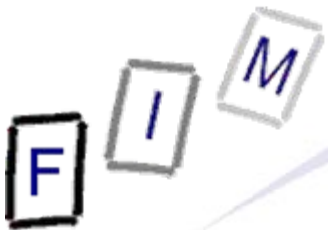
- Most offences are punishable only, when committed “without right” → General "exclusion" of liability/sanctions
 - Kind of “loophole” for countries
 - » If you don't want to punish it, provide for the person to have a right to do it (usually used for special cases only!)
- Examples of exclusion:
 - Consent (by the victim), self defense, necessity, ...
 - Lawful government authority
 - » For public order, national security, investigation of crimes, ...
 - Tools/acts for designing system, verifying security, ...
 - Common commercial practices (e. g. cookies, caches)



Substantive law



- Accessing the whole or any part of a computer system
 - Hacking passwords, using other person's passwords, employing an existing login, hacking a WLAN, ...
 - The intrusion itself is illegal, not only its consequences, e.g. damages, theft of data, privacy infraction, ...
- Required: Intentionally and without right
- Optional:
 - By infringing security measures
 - » Exclusion of unsecured systems allowed
 - Intent of obtaining computer data
 - » Not just "stealing CPU time"!
 - Other dishonest intent
 - » Like using the data obtained for gain/damage
 - In a computer system that is connected to another system
 - » Excluding stand-alone systems



- Access = Entering any part of the system
 - Retrieving some information (e.g. directory) from the system that would otherwise not be available
 - Excluded: Mere sending of data to system (e.g. mail or file)
 - » That is accepted by the system (or rejected)
 - Might be quite informative, e.g. success/detailed error message!
 - » Difficult: Sending mail reveals some information (= the computer accepts mails; version of MTA), which might be confidential (e.g. if it is not published anywhere: port-scanning)
 - Difference to sending a password and waiting for the response (valid/invalid) or "accessing a webpage" (included, but "with right")?
 - Requires the possibility to act within the system
 - » But not that any act is actually performed!
- Some security measures must exist and be infringed
 - Completely free computer is "free for access"!



- Interception by technical means of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions
 - Violation of privacy, related to data protection laws
 - “Non-public” refers to the transmission, not the content
 - » Public data sent privately is still protected
 - » Private communication over public networks can be protected
 - Individually selected and closed group of recipients
 - Electromagnetic emission is not included in “computer data”, but nevertheless protected
 - » Radiation of screens, wires, ...
 - WLAN is transmission of computer data
- Required: Intentionally and without right
 - Data retention → With right!

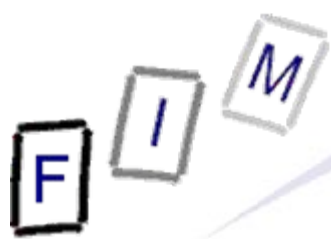


- Technical means: Through access to the system or through eavesdropping devices
 - Physical devices: Wire taps
 - Logical devices: Copying the transmission at an intermediary (switch, router, ...)
 - Just listening or looking when a person communicates is not included (un-technical means)!
- Recording / using the information is not required
- Optional:
 - » Intention: So it can be matched to illegal access, which is similar
 - Access: Device itself; Interception: The content within the device
 - Dishonest intent
 - In a computer system that is connected to another system



Data interference

- Damaging, deletion, deterioration, alteration or suppression of computer data
 - =Protecting the existence and integrity of computer data
 - Examples: Viruses, trojans, deleting/encrypting other's data
 - Anonymizers: Allowed
 - » Unless used to hide identity when committing a crime!
 - E.g: E-Mail anonymization might be legal, forging the sender IP address of a packet not
- Required: Intentionally and without right
- Optional:
 - Resulting in serious harm
 - » What is "serious" is for the countries to decide
 - » Intended to exclude small infractions



System interference / Computer sabotage

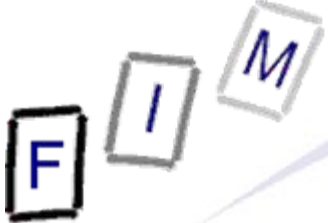
- Serious hindering of functioning of computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data
 - Protecting the usability of computer systems for their owner
 - Applies to computers and communication equipment alike
 - Examples: Viruses, (D)DoS, Ping of Death, Mail-bombs, ...
 - Not included is ordinary Spam
 - » Intention is **not** hindering comm., but to annoy, defraud, ...!
 - Hindering=Interfering with proper functioning
 - » "Serious": More than a slow-down/some restrictions; not working at all, extremely slow, accepting no more jobs, ...
 - » The level of harm required can be set by each country
- Required: Intentionally and without right



- Possession, production, sale, procurement for use, import, distribution, or otherwise making available of
 - a device (incl. program), designed or adapted primarily for purpose of committing any of the previous offences
 - » Tools to be used for criminal activity ("crowbar")
 - a password, access code, or similar data by which the whole or any part of a computer system can be accessed
 - » Information to be used to get access ("key")
 - with intent of committing any of the previous offences
 - » Mere possession alone is insufficient → You have to intend to use it for the criminal activity as well!
 - » Tools intended for computer security are therefore allowed!
- Required: Intentionally and without right
- Optional: Possession requires a minimum number of items
 - Easier proving the intentions
 - Production, sale, ... → One must always be enough!



- Distribution: Active (e.g. sending to a mailing list)
- Making available: Passive (placing on a webpage)
 - Includes link-lists to such devices/software
- Device: Hardware or Software
 - A virus is such a device; its possession therefore illegal
- “Primarily”: Dual-use devices are usually excluded
 - Assessment: Objective view of the device
 - Normal software that can be misused is excluded as well
- “Similar data”: Private/secret keys, ...
 - E. g. codes for decrypting Pay-TV (⇒ Illegal access)
- Examples:
 - Bug exploit software, WLAN cracking software
 - Not: WLAN scanner, wiretaps



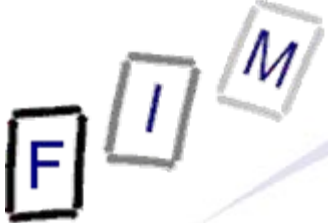
Misuse of devices: German BvG decision

- Decision by German constitutional court regarding the implementation law (§ 202c StGB; 18.5.2009, 2 BvR 2233/07)
 - That a tool can be used for a criminal activity is not sufficient
 - » Not even if it is especially suited for such activity
 - I.e., dual-use tools are not illegal, not even objectively
 - » This means, the intention of its owner is not even to be looked at
 - Trojans etc. will typically be such tools
 - » But investigating them (Antivirus producers) and teaching about them (university professors) is legal, as they don't intend to use them for a criminal activity
 - Such illegal tools may even be shared with specific other persons, regardless of their origin, if the recipient intends legal actions with it
 - » This requires e.g. documentation, authorization, etc.
 - » This does **NOT** allow to put them on the Internet!
 - You realize and accept that others might misuse them



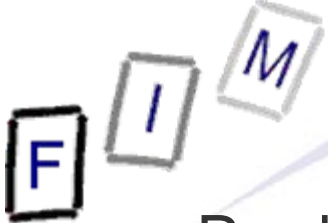
Computer-related forgery

- Input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered and acted upon for legal purposes as if authentic
 - Similar to forging (paper) documents
 - Readability/Intelligibility of data unimportant
 - » Independent of paper and eyes → Any code is sufficient
 - Deception can be on:
 - » Issuer: Who said this, i.e. "authorship"
 - » Genuine: Whether the content is correct; "truthfulness"
 - This is optional!
 - Legal purpose: To be used as evidence
 - » Not necessarily in proceedings; for any kind of legal action!
- Required: Intentionally and without right
- Optional:
 - Intent to defraud or other dishonest intent



Computer-related fraud

- Causing loss of property to another person by
 - any input, alteration, deletion or suppression of data
 - any interference with the functioning of a computer system
 - » Hardware manipulations, suppressing printouts, ...
- with fraudulent or dishonest intent of procuring an economic benefit without right for oneself or another person
 - “Interference”: Changing program, parameters, input, ...
 - “Loss of property”: Everything of economic value
 - “without right”: Disabling a webshop pursuant to an (e.g. unpaid) contract is allowed
 - Only purpose is loss to others, but no gain at all → Excluded!
 - » See data/system interference
 - Examples: Credit card fraud, using stolen ATM cards, ...
- Required: Intentionally and without right



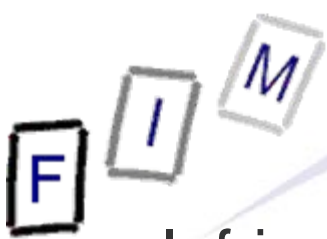
Content-related offences: Child pornography

- Production, offering, making available, distributing, transmitting, procuring, and possession of child pornography in a computer system or a computer-data storage medium
- Child pornography:
 - Minor (=under 18) engaged in sexually explicit conduct
 - Person appearing to be a minor in such conduct
 - » Actually an adult, but made to look like a child
 - Realistic images depicting a minor in such conduct
 - » Drawings, no human person involved!
- Required: Intentionally and without right
 - Right: For example medical use
- Optional:
 - Procuring and possession
 - No real minors involved
 - At least 16 years as lowest age-limit



Content-related offences: Child pornography

- "Offering": requires the ability to actually provide it
 - Just stating that you have it is insufficient!
- Making available: Placing it online (includes link lists)
- Possession: Debated whether online viewing is possession
 - Note: Possessing a link alone is insufficient
 - » But if you have a link, you probably have viewed the page ...
- Distribution: To a number of persons
 - Transmission: To an individual recipient
- Procuring: Actively obtaining
 - Regardless for what purpose, e.g. to tell the police → Illegal
 - Pop-up with illegal content → No procurement → Legal
 - » This is also no "possession", as the will to possess is missing!
- Sexually explicit conduct
 - Intercourse in all variations, bestiality, masturbation, sadism, masochism, lascivious exhibition of genitals/pubic area



Infringement of copyright & related rights

- Infringement of copyright and related rights as defined in the Berne convention, TRIPS (+...) when committed on a commercial scale and by means of a computer system
 - Only those parts of conventions in force in country!
 - What is an infringement of copyright is defined nationally!
 - » I.e. what a state declares as illegal, he must criminalize
 - » What he allows, he need not criminalize!
 - Excluded: Moral rights; i.e. only the "commercial" rights
 - Excluded: Patents, trademarks (not listed)
- Required: Willfully
 - Similar to intentionally; but this term is used in the convent.
 - Without right: Included in "infringement"!
- Optional:
 - In limited circumstances and only if other effective remedies are available and the conventions allow this



Procedure, sanctions, ...



Sanctions and measures

- Must be criminal law for natural persons
 - Effective, proportionate and dissuasive sanctions
 - Must include possibility for deprivation of liberty
 - Can be any type of sanction in case of corporate liability
 - Effective, proportionate and dissuasive sanctions
 - Must include possibility for monetary sanctions
 - Corporate liability: The legal person is held liable for a criminal offence committed for its benefit by a natural person with a leading position
 - » Power of representation, decision/control authority
 - » Includes liability for a lack of supervision/control, that made the offence possible by (any!) person acting under its authority!
- Extent is not prescribed!**
- Other measures are possible
 - E.g. forfeiture of tools, probation, injunctions, ...



- Jurisdiction over offences committed in
 1. the countries territory
 2. on board a ship flying the flag of the country
 3. on board an aircraft registered under laws of the country
 4. by a national: if the offence is punishable under criminal law where it was committed, or if committed outside jurisdiction of any state
- Optional: 2-4, any other jurisdiction desired
- Special jurisdiction related to extradition
 - Jurisdiction must be present when an alleged offender is present in a countries territory and extradition is denied solely on basis of nationality
- Other (additional) jurisdictions are possible
- These are quite standard rules and nothing exceptional!



- Multiple jurisdictions
 - "Consultation shall be done when appropriate, where prosecution would be most appropriate"
 - » Declining consultation possible if this would hinder investigation
- Location of an offence
 - Explanations only, but common understanding
 - Where the act is done
 - Where the result is achieved
 - » Example: Computer-related fraud: Person in A manipulates computer in B for loss of owner in C and benefit for person in D
 - » 4 countries would possess jurisdiction:
 - A: Location of acting
 - B: Location of modification of the data
 - C: Location of the victim
 - D: Location of abetting (only over D)



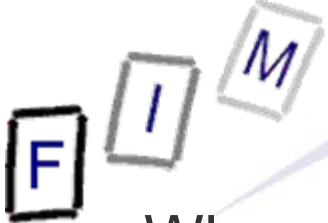
Expedited preservation

- Competent authorities must be able to order expedited preservation of specified computer data (incl. traffic data), which is possessed or controlled
 - Maximum period: 90 days (renewal possible)
 - No disclosure included: Separate laws!
 - » The preservation exists so that a (lengthy) procedure for disclosure can be started, which can later be fulfilled
 - » Otherwise: "Sorry, the data has already been deleted"
 - Only for a specific investigation (Art 14)!
- Custodian of the data must keep this order confidential for a certain time
 - Disputed: Employer of the person receiving the order also may not know about it!
- Subject to safeguards matching the ECHR
 - E.g. ind. supervision, requiring grounds, scope limitations, ...



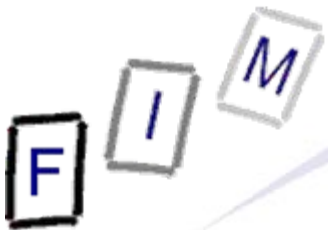
Preservation vs. Retention

- Preservation: Data already exists; prevent it from deletion
 - Applies to specific single persons; no data → no preservation
 - May be "copied out" to somewhere
 - » Privacy laws → Deletion obligation exists!
 - Requires a suitable initial suspicion from somewhere else
 - No real sense in reusing it
- Retention: Make sure data exists
 - Applies to all persons, regardless of suspicion/crime/...
 - Must be kept in its original form
 - Will probably soon be used for various other tasks
- Convention on Cybercrime
 - **No** obligation for monitoring and collecting: Only what is already there (because of various legal, business, ... reasons) must be preserved securely
 - Must be for specific case: Not generally or "just in case"



Partial disclosure of traffic data

- When data has been preserved (previous slides), a partial disclosure might be necessary
 - You only have the "last" IP address → Preservation there
 - But what about the steps before? Must be preserved too!
 - » Some disclosure is necessary to trace the complete connection and require preservation (and part. disclosure) there as well
- Problem: Often you just want the destination/source, which you get by this "emergency" measure, although you should only get it after disclosure was ordered e.g. by a judge!
 - Practice: You get the IP of all stages, but on the last stage, the identity is NOT disclosed → Wait for official grant
 - But: The IP is typically not the person → Procedure for name
- National law decides, how this is done
 - Single order (applicability decided by police; or each provider passes it on to the next), or separate orders for each step in the chain (time-consuming!)



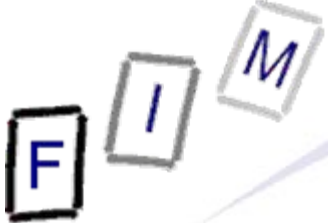
Partial disclosure of traffic data

- What is to be disclosed immediately: Sufficient traffic data to
 - enable identification of the service provider
 - » Where did you get the data from/where was it sent to?
 - enable identification of the path of the communication
 - » Any tracing information stored (e.g. routing data)
- Typical application: Tracing webmail
 - Large webmail providers know (log) the client IP address
 - » I.e., who user the web interface
 - » Need not appear in the E-Mail: Webserver appears as origin!
 - Preservation: Webmail provider
 - Partial disclosure: Actual source IP address
 - Tracing back: Preservation order to ISP of source IP address
 - » Note: No partial disclosure there (unless an anonymizer, ...)
- Subject to safeguards matching the ECHR
 - E.g. ind. supervision, requiring grounds, scope limitations, ...

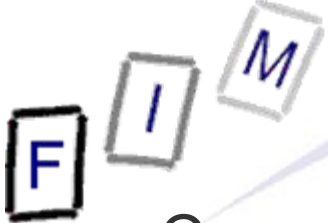


Production order

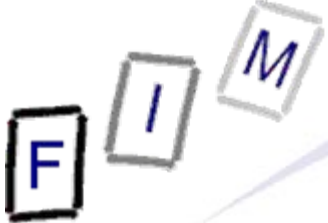
- Competent authority must be able to order
 - a person in its territory to submit specified computer data in that person's possession or control
 - » Seizure with the help of the person
 - a service provider offering services in its territory to submit subscriber information in its possession or control
 - » Tying communication end-points to persons
- Details:
 - Applies only to already existing data (no monitoring)
 - » Anonymous telephone service is still allowed!
 - » No obligation to guarantee correctness!
 - Control is more than "can access"; requires some right to it
 - » Like remote online storage, even when outside the country
 - Only for a specific case: Not generally or "just in case"
 - » Especially regarding subscribers



- Details:
 - Format of data can be set in order (e.g. disk or printout)
 - » Must probably be rather easily possible to be valid
 - » Extensive/Expensive conversions cannot be required
 - Subscriber information contains
 - » No traffic or content data
 - » User's identity, postal/geographic address, telephone number,...
 - » Billing and payment information (credit card data)
 - » Site or location of the equipment
 - » Assigned IP address (DHCP)
 - » E-Mail address, domain name
 - » IMEI, type of service (voice, fax, data, SMS, ...)
- Subject to safeguards matching the ECHR
 - E.g. judicial order required, content limitations, ...



- Competent authorities must be able to search or access computer systems, computer data stored in such, and storage mediums in its territory
- Seizure must be possible of computer systems, storage mediums, copies of data
 - Copy on other media, printouts, ...
 - Whole computer system, if access is otherwise impossible
 - » Strange operating systems/software/file formats/...
- Possibility of maintaining its integrity (access/write blocking) and rendering it inaccessible or removing it
 - Access/write blocks, encryption, changing passwords, seize media, ...
 - The current owner should no longer have access to it, but it is not completely destroyed
 - » Return after the proceedings should remain possible!



- Extension to other connected systems
 - All, which are lawfully accessible from or available to the initial system
 - » May require an extension of the warrant
 - » No problem: External storage device (e. g. backup)
 - **But** also included: **Any** remote account **anywhere!**
 - » Would be possible across several steps!
 - All systems must be on the countries territory
 - » This can be difficult/impossible to ascertain in the Internet...
- Ordering any person with knowledge about the functioning of the system or measures for its protection, when reasonable, to disclose this information to enable search or seizure
 - To overcome practical problems of access
 - » Typically system administrators
 - To ensure that the search is as quick an least disrupting to a business as possible



- Ordering a person to cooperate: Many problems!
 - Right to not incriminate yourself
 - » Only possible to third persons, not to the accused
 - Search orders: Customarily require only passivity
 - » No resistance; but not obligation to cooperate
 - Practice: Help to keep disruption minimal
 - The person who should help is often not involved
 - » Similar to an order to “anyone must help”, which is otherwise very rare/restricted
 - Passwords/Keys are often not restricted to the specific data sought: Could be easily used for other things too
 - » Master password: Not “reasonable”
 - Then it could be disclosure of only the data to be searched/seized!
 - Legal obligation relieves an administrator of contractual or other non-disclosure obligations!

Depends fully on shaping of “reasonable”!

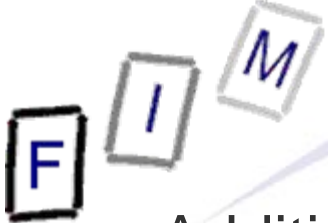


Real-time collection / Interception

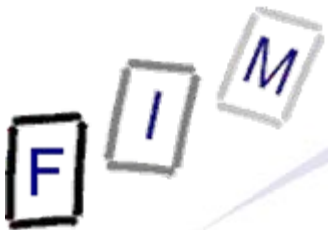
- Collection of traffic data: Itself or through service provider
 - Traffic data associated with specified communications transmitted by a computer system in real-time
 - Competent authorities, collecting by the provider, or the provider must cooperate and assist the authorities
 - Only within technical capabilities
 - » No requirement for "eavesdropping boxes", interfaces, ...
 - Provider must keep the fact secret
- Interception of content data: Similar as above
 - Only for **serious offences** (as determined by domestic law)
- Service provider must keep both the fact and any information relating to it confidential
- Similar to conventional wiretapping, but for computer comm.
- Subject to safeguards matching the ECHR



- Point of contact available 24 hours/7 days per week for immediate assistance in investigations and collection of evidence by
 - providing technical advice
 - preservation of data (see before)
 - collecting evidence, giving legal advice, locating suspects
 - » Legal advice: Only regarding the cooperation, preservation, ...!
- Either by carrying out the requests or facilitation
 - E.g. contacting the correct judges for issuing orders
- One of the main ideas of the convention!
 - Good idea, but rather costly: Highly trained (and expensive) personnel and equipment required!
 - » Practice: Database of the police headquarters
 - Rather restricted regarding what they will do
 - They know the phone number of the journal judge, ...



- Additional protocol; open to all Cybercrime convent. parties
 - In force since 1.3.2006; 34 signatures, 17 ratifications
 - Criminalizes racist/xenophobic material on computer systems
- Racist and xenophobic material is
 - Any written material, image, or other rep. of ideas or theories
 - which advocates, promotes or incites
 - » Scientific and "anti-" material is still allowed
 - hatred, discrimination or violence
 - against any individual or group of individuals
 - » Flaming a single person because of ... is sufficient!
 - based on race, color, descent, national-/ethnic origin, religion (when used as a pretext for any of the above)
 - » Note: Gender and "religion itself" are not included!
- In contradiction with the freedom of expression (ECHR)
 - Solution is the "normal" one: Every expression is limited by the rights of the others



Additional protocol: Racism (2)

- Specifically prohibited is
 - » Punishable if committed regarding persons for belonging to a group defined by any criteria above or regarding such a group
 - » All must be performed through a computer system
 - Dissemination: Distributing/making available of racist/xenophobic material to the public
 - » Does not affect "closed groups"!
 - Threats: With serious criminal offence
 - » National law defines, what a serious criminal offence is
 - Public insults
 - Denial, gross minimization, approval, or justification of genocide or crimes against humanity
- Required: Intentionally and without right
 - Optional: Almost everything (Not: threats!)



- A good approach to harmonize criminalization of certain acts in the computer area
- But suffers from typical problem of international treaties
 - Everyone wants an exception
 - No agreement on a single set
 - Many things remain optional or can be opted-out
- Additional protocol regarding racist/xenophobic material
 - Doesn't quite match: The convention is about specific acts, the protocol about specific content
- An important step, but largely depends on the national implementations
 - Which in many cases may take several years or even decades to be actually adapted/introduced

F I M

Questions?

Thank you for your attention!



- Convention on Cybercrime:
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
→ See also: <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>
- Explanatory report on Convention on Cybercrime:
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>
- Declan McCullagh: Cybercrime Solution has Bugs
<http://www.wired.com/news/politics/0,1283,36047,00.html>
- Politechbot.com (Contains comments):
<http://www.politechbot.com/docs/treaty.html>
- US DoJ FAQ on convention (DRAFT):
<http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm>