12. Social aspects of information processing

– large field
– but we restrict ourselves here to some ethical and legal aspects

12.1 Protection of privacy

= protection of persons and institutions against unrestricted acquisition, storing, usage and distribution of their personal data

Necessity follows from basic human rights:
- dignity and integrity of the individual is to be protected
- liberty and equal rights would be endangered if data are misused by authorities (cf. George Orwell: "1984" – "Big Brother is watching you")

in Germany 1983: Highest court decides *against* a census which was planned by the government because the survey was too deep – "informational self-determination" becomes practically part of the constitution

1990: United Nations ask all member nations to pass laws in order to protect privacy

1995: Privacy protection guidelines of the European Union

2000: Protection of privacy becomes part of the European charter of human rights

Protection of privacy is also a matter when only "conventional", non-electronic data are concerned (the "Stasi" in the GDR had only very low-level computers!)

but: with modern information technology, much more data can be acquired, processed, moved, distributed
→ greater temptation for misuse

Principles of protection of privacy:

- *legality*: ban against all data processing which violates human rights or man's dignity, ban against processing all data which was gained under deception

- *correctness*: processing of correct data, checking for correctness

- *determination by purpose*: use of data is only allowed for the purpose for which they were acquired

- *right to get information*: everyone shall know who has which data about him

- *protection against discrimination*: ban of processing sensible data (e.g., about sexual habits, ethnic affiliation, world view...)

- *informational self-determination*: The person affected can contradict the acquisition of his/her data, or (more strictly): The person affected must explicitely agree.

Problems:

- many exceptions to these principles in the laws of the nations and states, particularly when security questions are involved
  – degradation of privacy after 9/11

- often even sensible data are given voluntarily in the internet
  – danger of misuse grows with the advent of even more e-commerce applications and internet-based promotion

Recommendations for acquisition and use of data:

- *every data* can be sensible (under certain circumstances / for some persons) – be careful!

- use *no person-related data* or only a minimal amount

- *check the necessity* of all data already when you design a survey or a project where data are to be acquired

- if person-related data are necessary, store them on a computer *which is not connected to the internet* ($\rightarrow$ most effective protection against illegal intrusion)

12.2 Issues of computer security and integrity

- authentification by passwords
- illegal intrusion into foreign computer systems (by "crackers")
- computer viruses (and worms)
- spam

Authentification by passwords:
tool to restrict access to computers / networks / private data

- minimal requirement if several users work at the same computer / network
- not very secure!

often passwords were guessed or cracked using programmes which systematically try very many possibilities

Recommendations for passwords:

- use long enough words (6 characters minimum!)
- do *not* use just your boyfriend's/girlfriend's name, or the name of your cat/dog, or the like... these can be guessed *very* easily!
- mix letters with digits, or, even better, with extra symbols (%, @, &, $...)
- do *never* write your passwords into a text file on a computer (or on a palmtop, mobile phone...)
- change your password from time to time
- do not use the same password for all systems / computers
- do *never* share your password with other people (even if they seem trustworthy)

Illegal intrusion into a system ("cracking"):

- is in most nations forbidden by law
- severe punishments
- this is no trivial offence
- violates the personal rights and integrity of the owner of the computer, like conventional burglary
- very large damage was already caused by hacking computer systems containing sensible data

Refined version of intrusion:
by computer viruses (see below), using deception to get your password or credit-card number from you ("phishing")

Recommendation:
do *never* enter your password or CC number or other personal data into a window on the computer screen if you are not completely secure that the right application is running

Computer viruses:
pieces of computer code (machine code) which are able to replicate and spread to other computers

Difference between "virus" and "worm":
A virus needs a host programme to get executed.

Writing computer viruses is also *forbidden by law* and subject of punishment
– for good reasons: viruses can cause severe damage, even to systems where human lifes depend upon (e.g., computers in hospitals, power stations, air control...)

Recommendations:

- install a virus-protection software on your computer
- update it regularly (many systems provide the option for automatical update)
- be very careful with opening e-mail attachments (because they can contain viruses)
- do *never* open an e-mail attachment from a sender who you do not know or from a message which has no plain-text content
- check floppy disks, CD-ROMs etc. by your virus-protection software before you start loading something from them

Spam:

Advertisements or snowball-principle letters, lotteries etc. distributed by e-mail

- significant portion of all e-mails
- severe problem for the global e-mail exchange
- forbidden in many countries, but in others not → spammer can easily avoid legal consequences

Recommendations:

- use a spam filter
- do *never* answer to a spam message
    - if you want to order something in the internet, use serious e-commerce companies (you can find them using web portals like Yahoo, t-online etc. or using search engines)
- avoid to become a spammer yourself:

Do *never* react to e-mails which want you to forward them to all your friends (even if they come from a friend) – they are almost *certainly* based on hoaxes!
(Some computer scientists consider these hoaxes as a sort of viruses)

12.3 Property rights at programmes

Software that you can buy somewhere is – like most music, films, videos, books, games... – subject to *copyright*:

- The original code is *owned* by a person or (more often) by a company which has developed it (and often has invested much money into development).
- Initially, law guarantees the owner the exclusive right to use, copy, distribute, modify... his/her software.
- The owner can give away or *sell* the software together with a *licence* restricting its use and further distribution.
- If you want to use the software, you have to acquire it correctly and to agree to the licence conditions.

Ownership at software is very often violated by illegal copying (the same for music, films, games...)

- this can potentially be punished by law
- ethical problem: If you have yourself developed a software under great efforts, you maybe want to sell it, too, and will oppose illegal copying...

Two contrasting positions:

humans can only be motivated by the possibility to make money $\rightarrow$ it is necessary to protect ownership at software because otherwise no one would develop software only large companies can produce complex software $\rightarrow$ companies must earn enough money to become large the market is beneficial in every circumstance free competitors at the software market will finally produce optimal software at fair prices – "commercial philosophy"	humans are motivated when they have found a problem which fascinates them this motivation is best maintained when they have free access to the things they need to solve the problem $\rightarrow$ especially, *information* should be free $\rightarrow$ software should be free optimal software is not built using a top-down strategy by a large company ("cathedral principle") but by the free exchange of motivated people, each of them contributing what he/she can do best ("bazaar principle") – "hacker philosophy"

Examples for software developed under the commercial philosophy: All what is expensive... including Windows, Word, Excel, ...

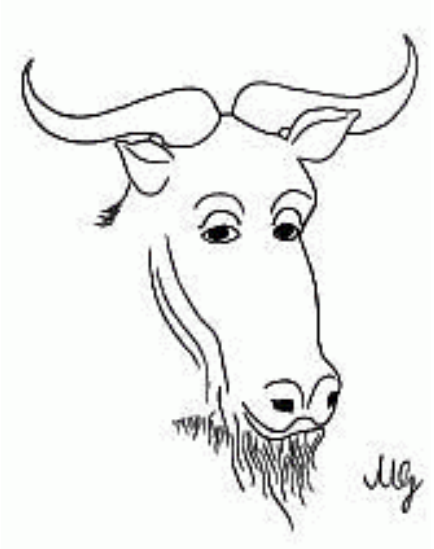
Examples for software developed under the hacker philosophy: Linux, FreeGIS, many tools distributed together with Linux...

- not yet decided which is better in the long run!

The GPL

In order to enable a "peaceful coexistence" of the two software worlds, the Free Software Foundation (promoting the "hacker philosophy" of software development) has designed a *licence* for *free software*:

The GNU General Public Licence (GPL).
GNU : a forerunner of Linux.



(GNU stands for "GNU's Not Unix".)

For the full text of this licence, see
`http://www.gnu.org/copyleft/gpl.html`

Principal points of the GPL:

"1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
> **(...)**

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange **(...)"**