Mag. iur. Dr. techn. Michael Sonntag

Privacy

Computer forensics

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

- Basics: See lecture “Legal basics for computer scientists”!
  - → The basic right
  - → Giving "consent"
  - → Exclusions
  - → …
- Here only some special topics:

Who is protected?

- EU directive: Only natural persons
  - → Austria: Extended to legal persons
- The intention is to protect humans from everything/-one else
  - → This includes:
    - » Children in relation to their parents
    - » Employees in relation to their manager/the employing company
    - » The managers from the public
  - → Excluded are:
    - » Anonymous persons
    - » Unique things
      - – Only as long as they are not associated with a single person!
- Legal entities are often protected only to a lesser degree
  - → See e.g. publishing financial data; or environmental pollution
  - → **They are included** in the (later) directive on privacy and electronic communications!

Identifiability

- Only persons identified or identifiable are protected
  - → If nobody can say who the person is the data relates to, there is no danger at all (purely statistical data)
  - → For the EU directive "nobody" means:
    - » Identification only through an external entity with no obligation to provide the information, like an ISP → Not identifiable
      - – Problem: The ISP itself? The police where the ISP must disclose it?
    - » Identification possible through own databases, from sources that are controlled, or where disclosure is obligatory → Identifiable
  - → Legally enforceable or practically possible → Identifiable
- Identification can be possible directly or indirectly
  - → E.g. one/more factors specific to physical, physiological, mental, economic, cultural, social identity
    - » "The blonde girl working in the accounting department"
    - » If there is only one a) young woman, with b) blond hair, c) in that department → Still identifiable

Identifiability: Pseudonyms

- Pseudonym:
  - → Partitioning data into an identifying part and a random number
    - » E.g.: Name, address, social security number, … + RND
  - → and other data + same random number
    - » Like surfing habits, credit rating, …+ RND
- Every person has access to only a single part
  - → One employee knows all about person number 4711
  - → Another employee knows, who person number 4711 is
    - » But no other fact about this person!
- Still personally identifiable data, but much more secure!
  - → At least two persons are required for compromising data
- Difficulty: Partitioning!
  - → The "other data" might in total already be sufficient to again identify the person!

Identifiability: IP addresses

- In computer forensics, you often only get the IP address
  - → Distinguishing between “internal” and “external” ones:
    - » Internal: You know/can find out which computer (→ user) this is
      - – Therefore this is clearly identifiable data
      - – Austria: Directly person-related data
    - » External: Static IPs → Through WHOIS owner can be identified
      - – Typically a company, not a person
      - – Without any further information, no identification possible
      - – Austria: **In**directly person-related data
- Attention: Depending on the content of the communication, everything can be completely different!
  - → Example: E-Mail is observed on the wire
    - » We don’t just have the IP of sender and recipient, but also their full E-Mail addresses, probably their names (content!), …!

What is protected?

- All data relating to a protected person
  - → Example: Hair colour, voice, letters, personal habits or preferences, income, sexual orientation, last breakfast meal, creditworthiness, …
  - → Regardless whether it is "important“/”public” or not
    - » Together with other data it might become important
    - » Everyone can determine the importance for them autonomously
- Result: If there is a list of "person" (identified somehow) and "attribute(s) of this person", the list is protected!
  - → Note: There is one additional data hidden here: Being on the list!
  - → Example: List of name and address
    - » Public data (taken from phone book)
      - – Practically unprotected and completely harmless
    - » Add the heading: "AIDS patients"
      - – Suddenly this list becomes much more dangerous!

What is protected?

- Special protection exists for more "dangerous" data:
  - → "Sensitive" data: Closed list
    - » Racial/ethnic origin, political opinion, religious/philosophical beliefs, trade-union membership, health, sex life
  - → "Criminal" data: Closed list
    - » Offences, criminal convictions, security measures
      - – Does NOT refer to administrative sanctions or judgements in civil cases (national law may include them, however!)
  - → These two areas are more strongly restricted, but numerous exceptions are still possible (see later)
    - » Requirement for laws introducing exceptions:
      - – Normal data: "public interest"
      - – Sensitive data: "substantial public interest"
- "Closed list": Only what is listed and nothing else
  - → "Standard" protection: Everything (no closed list!)

What is not protected?

- Data which is not processed and stored
  - → If immediately and automatically filtered out, no limitation
    - » This means, there must be no possibility of reconstruction/…!
- Example: Calculating statistics on network packet length
  - → You have to look at the packet (→ IP address, content, …), but all that is processed and stored is the length
  - → But not:
    - » Storing the whole packet for later statistics
      - – You could also look at its content!
    - » Statistics of packet length of a certain user
      - – IP address is processed to select which packets to investigate!

Exclusions from protection

- Some data/persons is excluded wholly from the applicability of the directive
  - → Matters outside the scope of the EU
    - » Excluded from the applicability in Austria in the law
- Not applicable in all points:
  - → No information, no objection, no supervision, …
  - → Areas:
    - » National/Public security: Police
    - » Defence: Military secret service
    - » State security, including the economic well-being of the state
      - – Includes the EU
      - – Examples: Secret service (terrorism; economic warfare)
    - » State activities in criminal law: Preventive measures
  - → Note: The ECHR still applies, i.e. all exclusions must still conform to it!

Personal usage

- Purely personal or household activity by a natural person
  - → What you are doing privately
  - → One reason: The state doesn’t want to regulate/prosecute this; take care of your own data and select the persons you give it to responsibly
- Examples:
  - → Personal telephone directory
  - → List of your friend's birthdays
- Usually there exists a further restriction:
  - → This data may not leave the personal area
  - → Gathering the data is only allowed with the consent of the data subject or from public data
- This is a restrictive exclusion: Public discussion (gazettes) of personal matters (celebrities!) doesn't match this exclusion!

Exclusions: Overview

- The basic right prohibits any use of personal data
  - → See above: This will not work in society
- Several exclusions exist, when personal data may be collected, used, stored etc.
  - → Typically transferring the data is much stronger restricted!
  - → Fewer exclusions exist for the more "dangerous" subsets of data: sensitive and criminal data
- In the EU directive the exclusions are very general
  - → National law can either define them in more detail, like in Austria, or leave it up to the courts
- In general, there is a weighing of interests between the person the data is about, and the person wanting to use it
  - → Some decisions of this weighing have been included in the directive as pre-determined results (and examples)!

Which countries law's are applicable?

- Each country regulates data processing within its boundary
  - → An establishment on its territory, where data is processed
    - » Multinational company: National law applies to each establishment separately, i.e. where it is physically located
    - » This does not depend on where the data logically belongs to!
      - – Usual delineation: Processing in a country without establishment Law from the country where the main seat is located applies
  - → An establishment outside the EU where international law dictates, that the law of this EU country is to be applied
  - → Established solely outside the EU but processing takes place on equipment within the EU
- Exclusion from applicability: Mere transfer
  - → Transporting data through the EU is excluded
    - » Any kind of "working" on or with it → EU law applies
  - → Example: Data sent from USA to China via Internet through London

Confidentiality obligations

- Anyone acting under the authority of the controller or of the processor, including the processor himself, may only process personal data according to the instructions from the controller (or when required by law)
  - → This ensures that the controller is legally responsible for (almost) every processing with his data
    - » If someone does something clearly illegal and not required, this is their own fault then (→ they become the controller)!
  - → Ensures that data is not misused by processors
- Typically requires also a contract clause for all employees
  - → "Personal data will only be processed according to the directions given and not be disclosed to third persons"
  - → Important: Personal knowledge is often unavoidable → This must be restricted (if possible: chatting!)

Rights of the data subject

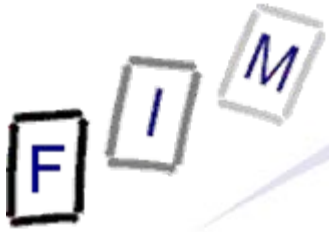
- The data subject has several rights
  - → Information, Access, Objecting (two different versions)
- Cannot be removed through contracts or terms of business
- Obligation of the data controller to enable them
  - → He need not provide incentives to do it
  - → He just isn't allowed to make it more difficult than necessary
- The data subject is obliged to cooperate
  - → Like providing the internal number of the processor if available to him ("customer number", …)
  - → Provide proof of identity
    - » Not: Using the right of access to get data on your neighbour …
- Restrictions are possible: National security etc.
  - → No access to your data in the police/secret service records!
  - → Correcting: Response is always the same “Was checked.”

Rights of the data subject: Information

- When collecting data, the following information must be provided to the data subject
  - » If the person doesn't have the information already
  - → Identity of the controller: Who am I?
  - → Purpose of the processing: What is intended
    - » Main reason: So the controller cannot use solely internal documentation of the purpose, which could be changed at a later point in time arbitrarily!
  - → Any further information required to fulfil the fairness principle
    - » (Categories of) recipients of the data
    - » Whether answering is obligatory and what the consequences are of not answering
      - – E.g. "Lottery ticket must be filled out completely or it is void"
    - » Existence of the right of access/correction
- See also "consent" above!

Conclusions

- Privacy is an important aspect in a free society
  - → Diverging interests must be balanced
- Currently privacy in on a constant decline
  - → Fear of terrorism
  - → "I have nothing to hide"
- Privacy legislation is quite strict and very effective in theory
  - → In practice it is often ignored to a large degree
  - → Only seldom infractions become known and are prosecuted
- Problematic are especially the security precautions
  - → Illegally selling data is rather rare, as far as known
  - → Illegally obtaining data (hacking) or losing it is common!
    - » Stolen laptops, unencrypted backup tapes lost, …



Questions?

Thank you for your attention!