

# Exemplary Privacy Cases

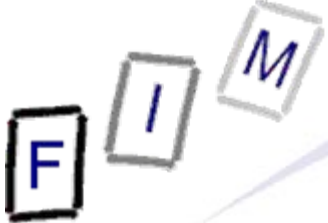
## Privacy law

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

E-Mail: [sonntag@fim.uni-linz.ac.at](mailto:sonntag@fim.uni-linz.ac.at)  
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



- EU privacy cases
  - Bodil Lindqvist
  - Promusicae
  - Huber
  
- What to do:
  - General presentation
  - Discussion
  - Read decision



- Miss Lindqvist works as a cleaning lady and in a church
- After a computer course she installed a homepage to inform all the church members on current events
  - She initiated a link from Swedish church homepage to hers
- Content of the homepage
  - » About her and 18 work colleagues from the parish
  - Complete name or only christian name
  - Employment or hobbies
  - Sometimes the family situation (married, ...)
  - Partly the telephone number
  - For some persons further information
  - One co-worker: She hurt her leg and is partially on sick leave
- There is no consent by these persons
  - After some complaints the pages were removed immediately



# Verdeckte Videoüberwachung

Die Klägerin war Kassiererin in einem Getränkemarkt, dem Beklagten, und dort auch für die Leergutrücknahme zuständig. Hierbei werden die Flaschen entgegengenommen, ein Bon ausgedruckt und mit diesem Bon erhält man dann an der Kasse Bargeld.

In diesem Bereich traten sein 1997 überdurchschnittlich hohe Inventurdifferenzen auf (Geldauszahlungen ohne vorhandenes Leergut). Es erfolgte eine Innenrevision, eine Überprüfung des Warenwirtschaftssystems sowie eine Überprüfung der Arbeitsabläufe. Es blieb jedoch nur mehr absichtliches Fehlverhalten als Grund übrig. Mit diesen Nachforschungen konnte der Kreis der Verdächtigen nicht näher eingegrenzt werden.

Im Jahre 2000 wurde daraufhin versteckt und heimlich eine Videoüberwachung der Kasse durchgeführt, später im Jahr auch in einem angrenzenden Gang, nachdem sich ein Verdacht ergeben hatte. Ob der Betriebsrat der Überwachung zugestimmt hat, wurde nicht festgestellt (gegenläufige Behauptungen). Aufgrund der Videoüberwachung wurde klar, dass die Klägerin Bons ausdrückte ohne Flaschen entgegenzunehmen, mit diesen Bons zur Kasse ging und dort das Geld entnahm. Anschließend begab sie sich damit in den Gang, wo sie das Geld einsteckte.

Darauf hin wurde sie mit Zustimmung des Betriebsrates fristlos entlassen.

**Klagebegehren:** Die Klägerin begehrt die Feststellung der Unwirksamkeit der Entlassung und die Nachzahlung entgangenen Lohnes.

## Varianten:

- 1) Die Videoüberwachung wurde heimlich eingerichtet (Betriebsrats-Zustimmung liegt vor) um eine allgemeine Produktivitätsüberwachung durchzuführen. Hierbei wird zufällig dieser Betrug aufgedeckt. Differiert das Ergebnis?
- 2) Wie Variante 1, aber diesmal wurde der Betriebsrat nicht befasst (dieser hat keine Kenntnis und daher auch keine Zustimmung abgegeben).

Welche Rechtsfolgen könnte die Videoüberwachung in den Varianten noch hervorrufen?



- The public prosecutor started proceedings because of
  - Automated processing of personal data without previous notification of the "Datainspektion"
    - » Datainspektion = The Swedish privacy commission
  - Processing sensible data without prior permission
    - » Collecting and putting it in the webpage, publishing the webpage on a webserver
  - Export of personal data to third countries without permission
    - » I.e., publishing on the Internet (accessible from everywhere)
- First instance: Penalty of  $\approx$  € 450,-



- What the Swedish supreme court asked the ECJ:
  - Is mentioning the name of a person on a webpage a privacy matter? Is this "automated processing of personal data"?
  - Is mentioning a leg injury/sick leave medical (=sensible) data?
  - Is publishing on the Internet a transmission abroad?
    - Swedish person puts Swedish data on a Swedish server
      - » Is it important whether some foreign person accessed it?
      - » Is it important where the server is located?
  - Are the directive restrictions compatible with the ECHR?
  - Can a country institute more stringent protection laws?
- Note:
  - The facts are undisputed
  - What is at issue is solely their legal evaluation!



- What exactly is personal data?
  - Where is the delineation to anonymous data?
  - What of the data listed is "personal data"?
- What about purely personal data processing?
  - What is it? Is it applicable here?
- When is data processing "automated"?
- What is data "concerning health"?
  - Is this to be seen narrowly or extensively?
- When a web server is accessed from other countries, how does this happen technically?
  - How technically exports the data?
  - What is a physical comparison to this?



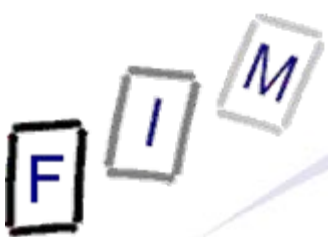
# Bodil Lindqvist: Aspects to consider

---

- The EU is not (yet) member of the ECHR
  - What about those rules? Are they applicable?
- What is "harmonization"?
  - Does this mean that all countries must do the same?
  - What's the difference between "directive" and "regulation"?
  - Define the scope of the directive with regard to national laws!



- Promusicae is a non-profit organisation of producers and publishers of musical and audiovisual recordings
- Applied for preliminary measures against Telefonica
  - **Telefonica: Huge telecomm. company, also an ISP**
- They asked for the identities and physical addresses of persons they provided Internet access to:
  - **Only IP address and date/time of connection were known**
  - **Allegedly these persons used the KaZaA file exchange program and provided access to music, for which Promusicae owns the exploitation rights**
- The typical filesharing case: IP address is known, and the user's identity needs to be obtained from the ISP for further (civil) legal proceedings against them

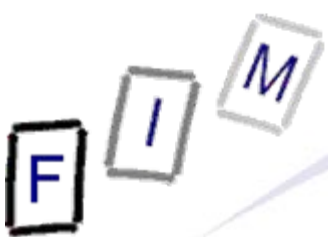


- Promusicae claims, these persons engage in unfair competition and infringe intellectual property rights
- Telefonica was unwilling to provide the information:
  - Authorisation for disclosure only in criminal proceedings
  - Privacy protection of their users
- Note: Telefonica does have the information and could provide it, if ordered to do so
  - They just think, that under Spanish law they are actually **forbidden** to provide it!
- Spanish law (Art. 12 para 3 Ley 34/2002 11.7.2002)

The data shall be retained for use in the context of a criminal investigation or to safeguard public security and national defence, and shall be made available to the courts or the public prosecutor at their request. Communication of the data to the forces of order shall be effected in accordance with the provisions of the rules on personal data protection. (Translation probably by EuGH)



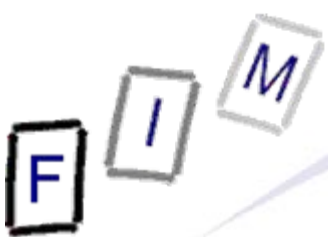
- Does the community law because of [several IP directives] permit member states to limit the disclosure duty of traffic data to criminal proceedings?
    - I.e., **must** there be a possibility to obtain the identity of a person from an ISP for a **civil** case?
  - Whether the storage of the information is in compliance with EC law (→ Telecom privacy directive!) is **not** an issue!
  - Note: **All three** IP directives listed **explicitly** do **not affect** any privacy requirements!
    - There is no explicit requirement for civil proceedings in there
    - But: States must ensure "effective protection"
      - » How they do this is (in a wide range) their own decision!
- Actual question: Disclosure vs. privacy!**



# Promusicae: Aspects to consider

---

- "Privacy" is a fundamental right
  - But so is "property" (including intellectual one),
  - and also "effective judicial protection"!
- What to do when several fundamental rights collide?
  - Laws (directives) might provide guidance
  - What is the role of EC law in this area?
- If a directive leaves an area open → What must states do?
  - Can they do everything?
  - Can they do nothing?
  - How is their freedom curtailed?
- What does Art. 42/47 of TRIPS really say?
  - Promusicae explicitly relies on it!
  - How does this "act" come in and what is its legal value?



# Promusicae: Aspects to consider

---

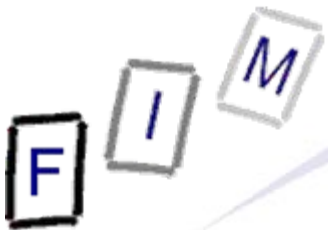
- Providing personal data to a third party: Isn't this what Promusicae wants?
  - What are legal requirements for this?
  - Do they match (or what provision would match best)?
    - » Is there place for this in the light of Spanish law?
- Three options identified by court; to be investigated in this order until a matching one has been found:
  - Is a law for such disclosure prohibited by EC law?
  - Are the member states required to provide such disclosure?
  - Do other EC laws require a different reading of the three IP directives?



- TRIPS = Agreement on Trade-Related Aspects of Intellectual Property Rights
  - Part of GATT ( prerequisite for membership in WTO – World Trading Organisation) since 1994
- *42 Fair and Equitable Procedures*

Members shall make available to right holders civil judicial procedures concerning the enforcement of any intellectual property right covered by this Agreement ...
- *47 Right of Information*

Members may provide that the judicial authorities shall have the authority, unless this would be out of proportion to the seriousness of the infringement, to order the infringer to inform the right holder of the identity of third persons involved in the production and distribution of the infringing goods or services and of their channels of distribution.



# Promusicae: Aspects to consider

---

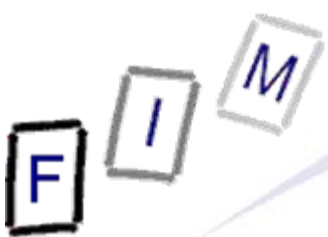
- What are the exceptions for processing traffic data in the telecommunications privacy directive?
  - What are the exceptions in Art 15 of the directive?
    - Art 15: Member states may restrict 95/46/EC (=privacy dir.) certain parts of the directive when necessary, appropriate and proportionate within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.
  - How do they compare with the general privacy directive?
    - Art 13 Abs 1 95/46/EC: Restriction when necessary to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, [...] the protection of the data subject or of the rights and freedoms of others.
  - What conclusion can be drawn from the difference?
  - Who could receive data then? Why is this?



- Mr. Huber is an Austrian national, but a resident in Germany
  - He is a self-employed insurance agent
  - His data is stored in “Central Register of Foreign Nationals”
    - » “Ausländerzentralregister – AZR”
    - » Central → Once for all of Germany
  - This data is available to numerous other authorities
- No specific problem exists
  - He just doesn’t like his data to be in this register
- Discrimination by nationality: Germans are **NOT** in there!
  - There exists an additional “normal“ residence register where everyone is in (including Germans), but this contains less data and is distributed (each municipality; ≈ 7700!)



- Content of the register
  - Name, given name, date/place of birth, nationality, marital status, sex
  - Passport particulars
  - Residence status
  - Record of entries into/exits from Germany
  - Records of previous statements as to domicile
  - Particulars about the authorities which supplied the data above and their reference numbers



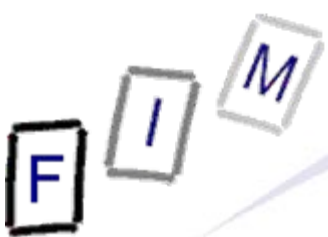
- Deletion request was denied by the administrative authority responsible for maintaining the register
  - Challenge against this was unsuccessful
- Administrative court (=3rd instance) decided that the storage and processing of the data was against EC law
- The Federal Republic of Germany appealed this decision
  - Higher administrative court (4th instance) sent it to the ECJ
    - » “Freedom of movement” is a central EC aim!
    - » It also includes a “non-discrimination” requirement



- Is it necessary to specially monitor foreigners residence?
- Does it really improve security to cover all (foreign) citizens, not only those with expulsion order/residence prohibition?
- Is the register an restriction of his right of free movement?
  - Which includes the “framework of conditions for an activity”!
- The “necessity” in the directive: Is it to be understood alone or must it be “filled” by the national legislation?
  - Can “administrative simplification” be a justification for such data processing?



- The register is also used for:
  - Asylum, statistical purposes
  - Exercise of security, police services
  - Prosecution and investigation of activities which are criminal or threaten public security
- Processing of personal data concerning public security, defence, state security and the activities of the state in areas of criminal law is expressly excluded from the directive!
  - But are **only** foreigners criminals?
- Discrimination:
  - Different situation → No discrimination possible?
    - » Germany, Netherlands, Denmark argued this
  - Different situation + difference relates and is proportional to difference in situation → No discrimination
    - » EU commission, court reporter



# Huber: Aspects to consider

---

- Which data is necessary for ascertaining a residence right?
  - Identity, employment/study documentation, evidence of financial resources
    - » Closed list from a different directive!
- Systematic and centralised vs. distributed register?
  - Not an equal treatment, may foster prejudice
  - Note: A centralised system as such is no problem at all!
- Does a statistic require personal data?
  - Count who enters and who leaves; storing it necessary?
- “Necessity” = “a pressing social need” + proportionality



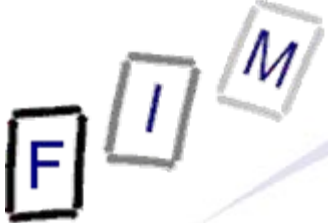
- Such a register does not satisfy “necessity”, unless
  - it contains only data necessary for the application
  - it is used only by the authorities responsible for the application
  - its centralisation enables the legislation to be more effectively applied as regards the right of residence
- Whether this is the case the national courts must decide
- This is never true for a statistical purpose
- This is never true for the purpose of fighting crime
  - Note: Because it **only** contains foreigners; fighting crime **must** take place against **all** nationals, including Germans!



# Non-Discrimination in free movement

---

- Comparable situations must not be treated differently
- Different situations must not be treated the same way
- Any difference may be justified only if it is
  - based on objective considerations
  - independent of the nationality of the persons concerned
  - proportionate to the objective being legitimately pursued



- Very few court decisions on privacy on European level
  - More on national level, but also not too numerous
- Bodil Linqvist:
  - The Internet may be international, but putting data on it is no export → This can be problematic!
    - » Note: Publication rights are still required!
  - Personal data is to be seen extensively and in favour of the data subject in all aspects
- Promusicae:
  - Disclosure of personal data to third parties is severely restricted, but much more lenient towards the state
  - States can "modify" privacy, by providing rights on data
    - » But they need not → This is their own decision
- Huber:
  - Data must be "necessary" → Not just helpful or "just in case"

F I M

# Questions?

Thank you for your attention!