Voluntariness of Permissions Required for Security Measures

Euromicro 2004, Rennes, 31.8.-3.9.2004

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

© Michael Sonntag 2004
Introduction

- Security measures are a necessity for every company
- Legally seen this is no problem on principle
  - Each company can decide who is allowed to do what with its own assets (machines, products, computers, ...)
  - However, actually verifying compliance can be a problem
    » As long as only the items alone are "verified" ⇒ legal
  - But very often this also gives information about the persons handling these items
    » E.g. tracking a lorry also tracks the person driving it
    » E.g. bodily searches prevent theft, but are very intrusive
- When security measures infringe personal rights, it's difficult
  - In the contract from the start: Slightly less difficulties than when introducing them later!
- Two "layers": Security measure itself & introducing it
Voluntariness: Usually discussed/defined through its opposite
   - Force: Directly influencing the actions
   - Threat and duress: Influencing the decision how to act
   - Lack of information: Withholding grounds for the decision

Depends on the context, but some common features/rules
   - Means, purpose and their relation
   - Information requirements

However, the standards and details are different
   - Criminal law: Rather strict (e.g. permission to injure)
   - Civil law: Rather loose (private autonomy)
   - Employment law: Third persons involved (work council)

Sometimes giving permission is even forbidden
   - E.g. Video surveillance of restrooms
Voluntariness of Permissions Required for Security Measures

Contexts of voluntariness: Criminal law

- No offence exists if the action was permitted by the "victim"
- Example of missing voluntariness: Compulsion
  » Principle applies everywhere but is most clear in this area!
- Three possibilities for non-voluntariness (of the act itself!)
  → Illegality of means: The security measure itself is illegal
    » Example: Searching employees homes for stolen computers
      – Extremely rare, especially for security measures!
  → Illegality of purpose: Aim of the measure is illegal
    » Example: Scanning E-Mail for political attitude
      – Only possible if the security measure is only a pretense
  → Illegality of relation: Huge measure for small purpose
    – Common, but most difficult area
    » Goal unattainable (e.g. bodily searches for laptops)
    » Quantitative problem (e.g. bodily search for stolen stamp)
    » Qualitative problem (=unrelated issues)
Voluntariness of Permissions Required for Security Measures

Contexts of voluntariness: Civil law (1)

- Practical influences on the decision are more free here
  - Economic, moral, psychologic, etc. pressure is no hindrance
- New aspect: Monetary equivalence of the exchange
  - Differs from illegality of relation: parties, not measure/goal!
  - Larger inequivalence ⇒ More strict assessment of voluntariness
- Several possibilities to remove voluntariness (introduction!):
  - Absolute force: Overrules the will of the acting person
    - Example: Moving someone other's hand. Not applicable here.
  - Duress: Influencing the intentions
    - External influence (Examples: threat of dismissal or pay cut)
      - Sometimes even if made by third parties (e.g. other manager)!
    - Reality of the fear: Objectively and subjectively measured
      - Usually no problem here!
    - Unjustness: See criminal law (measure, goal, their relation)
      - E.g. ordinary dismissal vs. transfer to a post without security risks?
Exploiting a quandary: Third party influences the decision

» Quandary (difficult situation): Seen subjectively
  – Example: Fear of dismissal (no new job: general quandary)
  – Example: Mortgage problems upon pay cut
  » Exploiter must know or should have known of it
  – In security rather rare: Will usually not be obvious

» Imbalance between performances of parties

• Imbalance is rather difficult here:
  » The quid pro quo of the worker is easy to determine
  » Personal information can even be calculated in money
  » The contribution of the company is, however, very difficult
  » Continued existence & welfare of company, secure workplace?

• Might not be applicable regarding disadvantages which cannot be assessed in money
  » Duress remains!
Voluntary consent

- Consent usually has no form requirements
  - But e.g. sensible personal data requires "explicit" consent
  - Better acquire it in writing (also as evidence)
- In contrast to the negative definitions above, some constitutive positive requirements will be discussed now
  - Information: No real free will possible without information
  - Freedom: The means/purpose relation exists twice
    » Measure: Security measure vs. intended security enhancement
    » Introduction: Security enhancement vs. "incentive" for consent
  - Special groups:
    » Underage persons are especially protected
    » External persons cause slightly different problems
A consequence of private autonomy is to forego information

- But without at least some information, the decision that no further information is needed is impossible!
- Therefore many protection rules exist
  - E.g. assistance obligations resulting from a work contract

More information is required, when

- the person cannot reasonably assess the security measure
  - E.g. what data is collected & what could be derived from this
- the measure is more in the interest of the company
  - E.g. protecting the companies infrastructure instead of protecting workers from liability for mistakes

Less information is necessary

- for remote/weak dangers (too much information otherwise)
- for illegal derivations/results (reduced, not removed!)
Voluntary consent: Freedom

- Relation of measure/security improvement is the difficult part
- Legality can be assessed e.g. by the following aspects:
  - Low degree in area A can be compensated by high degree in B
    → Importance of the purpose
    - Protecting less valuable resources requires more safeguards
      – Example: Protecting plans of future vs. very old products
    → Less intrusive alternatives
    - Only the least intrusive of equal measures is allowed
      – Example: Personal vs. automatic scanning of E-Mails for viruses
    → Suitability/probability for success
    - Rather ineffective measures are more easily illegal
      – Example: Logging logins to detect unauthorized physical intrusion
    → Tracing vs. detection vs. prevention
    - Prevention is best, tracing worst (many safeguards/high value/…)
      – Logging all web traffic vs. notifications vs. automatic blocking
Voluntary consent: Underage and external persons

- Security measures also apply to e.g. trainees
  - They don't have full legal capacity, so consent is difficult
  - However, certain personal rights can be disposed already at a lower age (Austria: e.g. choosing the religion ≥14 years)
  - Still, young employees will often lack insight into potential and intangible drawbacks,
    » More information required and less pressure allowed!

- "Transient subjects" of monitoring
  - Examples: service personnel, loan workers, guests
  - Consent is also required from them
  - Information requirements are lower
    » Dangers for them are less (short time, not own employer, ...) 
    » They pose more danger, so importance of measures is higher
  - But: They have much less interest in the security measure
Example: Filtering personal E-Mail

- No obligation to allow private use of E-Mail, WWW, ...
  → But usually allowed to some extent
- Still, filtering for viruses, spam, trojans, spyware, ... required
  → Personal information ⇒ protected even from processing

- Information requirements:
  → How and for what is scanned
    » "Undesired" content: Exact description; reason required
    » Automatic filtering and blocking (not deletion!): No problem
    » Personal verification: Only with additional restrictions!
  → What to do on wrong classification
    » Should be possible to "unblock" without another person

- Means for introduction
  → Permitting private use
    » Forbidding previously allowed private use sometimes difficult!
Intrusion detection systems monitor internal network traffic

- Similar in some way to permanent video surveillance
  - Can be misused to monitor employees' activities

Two main approaches:

- Signature detection: Searching for specific signs
  - False positives rare, consent easily possible
- Anomaly detection: Comparing to previous usage
  - Data must be stored, false positive rate higher
  - Personal verification of alerts required
  - Consent rather difficult (Austria: work council required)

Pseudonymous auditing might help

- Not anonymous \(\Rightarrow\) consent still required
- Personal verification without knowing who data is about
  - Consent can be given more easily (i.e. without work council)
Conclusions

- Security measures are a problem for real voluntariness
  - Only one side profits from them, the other very much less
  - Especially when introducing them later
    » Already in the contract: Salary is the benefit of the employee
- Common aspect are measure, goal and their relation
  - 1: Security measure and what it should achieve/protect
    » Mostly no problem (or technically possible to adapt so it isn't)
  - 2: "Incentive" for consent and introduction of the measure
- E-Mails:
  - Scanning: what to search for influences legal possibilities
  - Depends on actions and procedures for (false) positives
- IDS:
  - Depends on the type (signature: ✓, anomaly: ?)
  - Additional precautions required or consent difficult
Questions?

Thank you for your attention!