

I. Introduction

1. Privacy

1.1 Definition of Privacy:

Alan Westin (Columbia University, 1967):

" the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"

3 Dimensions of the Concept of Privacy:

1.) **privacy of person:**

- protecting a person against undue interference, such as physical searches and information that violates his/her moral sense.

2.) **territorial privacy:**

- there is a physical area surrounding a person that may not be violated without the acquiescence of the person(safeguards: laws referring to trespassers search warrants)

3.) **informational privacy:**

- deals with the gathering, compilation and selective dissemination of information

Basic privacy principles:

- lawfulness and fairness
- necessity of data collection and processing
- purpose specification and purpose binding
(there are no "non-sensitive" data)
- transparency =>
 - data subject's right to information / correction, erasure or blocking of incorrect/ illegally stored data
- supervision (-> control by independent data protection authority) and sanctions
- adequate organisational and technical safeguards

Privacy protection can be undertaken by

- privacy and data protection laws promoted by government
- self-regulation for fair information practices by codes of conducts promoted by businesses
- privacy-enhancing technologies adopted by individuals
- privacy education of consumers and IT professionals.

1.2 Privacy Risks at Application Level:

Collection / Transmission of great quantities of personal data:

Projects for new Applications on Information Highways, e.g. for:

- Health Networks
- Public administration Networks
- Research Networks
- Electronic Commerce
- Teleworking
- Distance Learning
- Private use

Example:

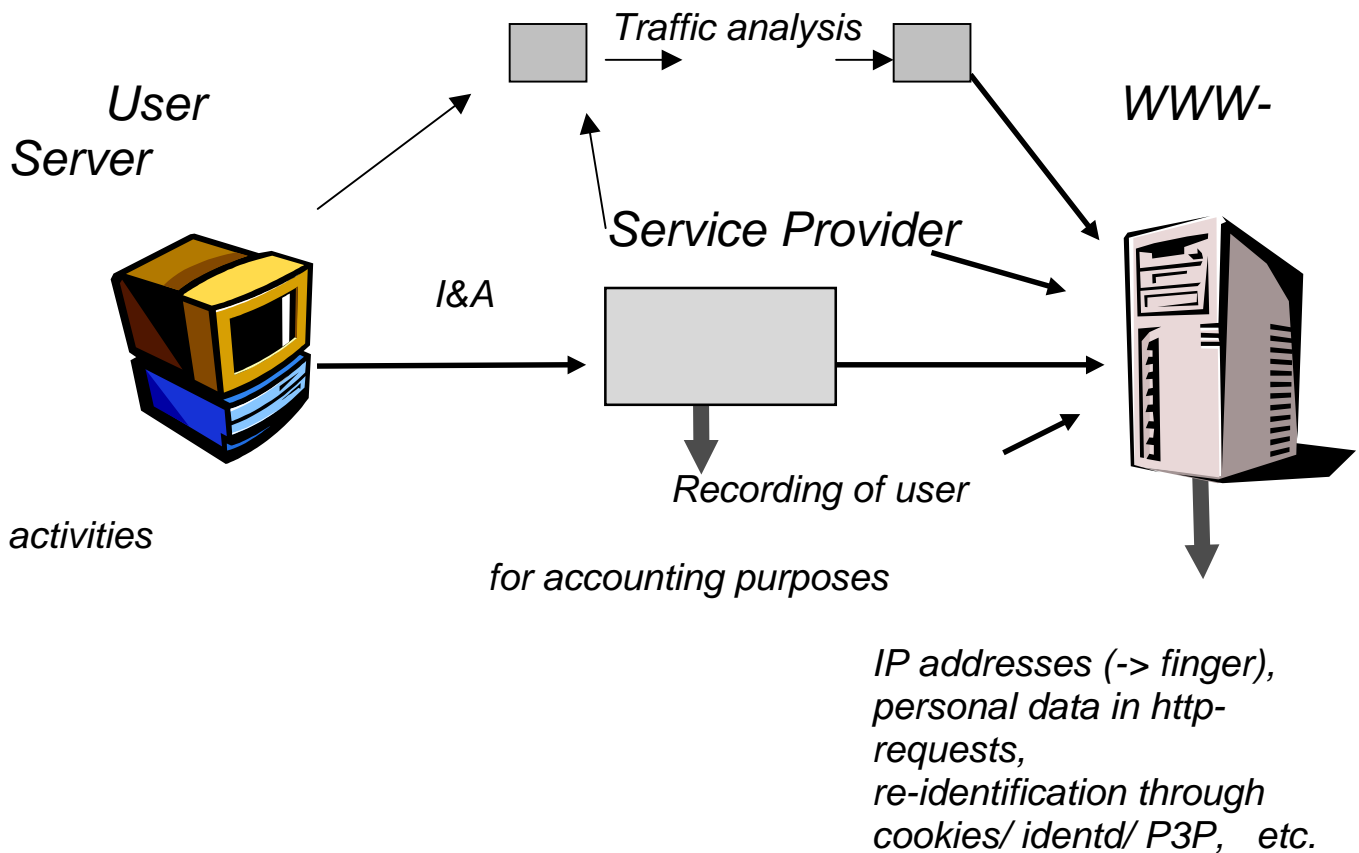
Information Infrastructure Initiatives for a better Health-Sector (see Danish "INFO-Society 2000"- or Bangemann-Report):

- Nation-/ European- wide Health Network for the Interchange of Information
- Interchange of (standardised) Electronic Patient Case Files
- Systems for Tele-Diagnosing and Clinical Treatment

1.3 Privacy Risks at Communication Level:

Anonymity of communication endangered:

Monitoring / Logging of Transactional Data



=> Creation / long-term storage of personal profiles possible

-> Privacy is an International Problem !

Example of a Netscape cookie file:

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.

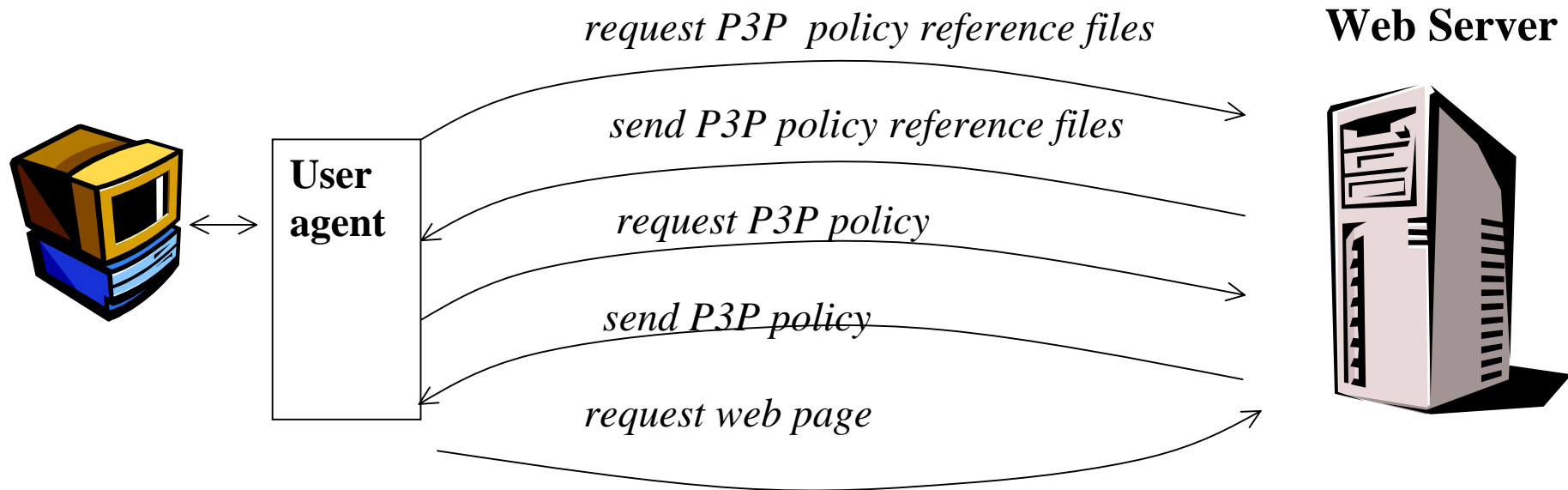
.doubleclick.net TRUE / FALSE 1920499140 id 5e47d2c
.excite.com TRUE / FALSE 946641600 UID 7A152CF333943ED8
.nrsite.com TRUE / FALSE 946598400 NRid iafC-yaFExOAgSq49wLzNq
.infoseek.com TRUE / FALSE 897052931 InfoseekUserId
056BEAA0F18BCF114413D6815EF2E721
.netscape.com TRUE / FALSE 946684799 NETSCAPE_ID
10010408,11761a29
www.aztech.com.sg FALSE / FALSE 1293753600 EGSOFT_ID
134.100.7.163-3531300016.29139179
.yahoo.com TRUE / FALSE 915145200 Y v=1&n=btderittbe9r7k
www.geocities.com FALSE / FALSE 937399384 Geold
13424395874327384530
.linkexchange.com TRUE / FALSE 942191999 SAFE_COOKIE
341d2eea1807d56e
.imgis.com TRUE / FALSE 1032612266 JEB2 -1869117967|
.focalink.com TRUE / FALSE 946641600 SB_ID
087753434900000738770889195370
.amazon.com TRUE / FALSE 2082787201 ubid-main 3826-5903423-
539594
www.csc.dk FALSE / FALSE 1293753600 EGSOFT_ID 134.100.7.163-
724676368.29159492
www.uk.uu.net FALSE / FALSE 946684799 INTERSE
134.100.7.16322729879443306351
www.hgs.se FALSE / FALSE 946511999 RoxenUserID
0x801292b9
www3.haaretz.co.il FALSE / FALSE 1293753600 EGSOFT_ID
134.100.7.163-2616727280.29163945
.preferences.com TRUE / FALSE 1182140421 PreferencesID
e9NFtWp8ioK5eo100BWHMa
.amazon.com TRUE / FALSE 885196800 session-id 9947-8202030-
317488
.amazon.com TRUE / FALSE 885196800 group_discount_cookie F
.amazon.com TRUE / FALSE 885196800 session-id-time 885196800
```

Cookie-Technology violates

- Art. 6 (*principles of accuracy, timeliness*)
- Art. 7 (*requirement of informed consent*)
- Art. 10 -12 (*information and access right*)

of the EU-Directive on Data Protection

Platform for Privacy Preferences (P3P):



User agent has to:

- request P3P policy reference file
- request P3P policy
- match policy with user preferences
- accept/ reject/ inform/ warn

Indication to P3P policy reference file through:

- well-known location (/wc/p3p.xml)
- html link tag
- http header

P3P privacy problems:

P3P alone does not fulfil the following EU-Directive requirements:

- Legitimacy (Art. 6b)
- Adequacy (Art. 6c)
- Right of Access (Art.12)
- Adequate level of protection for transborder data flow

Are users forced/pushed to give-up privacy ?

1.5 Problem of International Harmonisation of Privacy Legislation:

Is a common harmonised approach to privacy possible due to cultural/ historical/ political differences ?

European Union:

Privacy Regulations:

- EU Data Protection Directive 95/46/EC
 - EU Telecommunication Data Protection Directive 97/66/EC
 - Proposal for a EU Directive for privacy/data protection in the electronic sector
-
- instrument for harmonisation inside Europe
 - coercive effect on countries outside Europe
(->Eastern Europe, Quebec, Canada)

EU-Directive on Personal Data Protection:

EU-Directive on Personal Data Protection:

Objective (Art.1):

Protection of fundamental rights, freedoms, privacy rights of natural persons with respect to personal data processing

Personal data: information related to identified or identifiable natural persons

Scope (Art.3):

Processing of personal data wholly or partly by automatic means or of personal data that shall form a part of a filing system

Directive does not apply to processing of personal data

- for public security, defence, state security, activities of the state in the area of criminal law
- of a natural person for a purely personal activity

No distinction between private and public sector

Further Regulations:

- purpose specification and purpose binding (Art.6 I b)
- Necessity of data processing (Art.6 I c, Art.7)
- Identifiable form no longer than necessary (Art.6 I e)
- On principle no processing of special categories of data (Art.8)

- Data subjects have the right
 - to be informed (Art.10)
 - to be notified, if data have not been obtained from the data subject (Art.11)
 - of access to data (Art.12 a)
 - of correction of incorrect data / erasure or blocking of illegally stored data (Art.12b)
 - to object (Art.14)

- Security of processing (Art.17)

- Restriction of transfer of personal data from EU-countries to third countries (Art. 25)
 - Supplementary Codes of Conducts (Art. 27)
 - In each member state independent authorities shall supervise the protection of personal data (Art.28)
 - Supervisory authorities shall monitor compliance, act upon complaints, be consulted when drawing up data protection regulations, draw up regularly reports
 - Supervisory authorities shall be endowed with
 - investigative powers
 - effective powers for intervention
 - the power to engage in legal proceedings
 - Supervisory Authorities:
 - have to be notified about every plan for automatic data processing (Art.18, 19)
 - shall assess possible risks prior to the start (Art.20)
 - shall keep a register of operations (Art.21)
- simplification / exemptions, if controller appoints a "data protection official"

U.S.A.:

Privacy Regulations:

- no data protection commissioner
- no omnibus privacy legislation

Public Sector: U.S. Privacy Act (1974)
+ Privacy acts of the states

Private Sector: "patchwork": Fair Credit Reporting Act, etc.
self-regulation (-> codes of conducts)

→ USA does not provide adequate level of data protection as required by Art.25 EU Directive

Safe Harbor Privacy Principles as a solution ?

Safe Harbor Privacy Principles – issued by US Dept. of Commerce on July 21, 2000

Goals:

- to ensure high data protection standards while maintaining free flow of data
- to fulfil EU-required “adequacy standard”

7 Principles of data protection concerning:

- Notice
- Choice
- Onward Transfer
- Security
- Data Integrity
- Access
- Enforcement

Organisations can voluntarily join Safe Harbor by self-certification

Criticisms:

- Notice “as soon thereafter it is practicable”
- No requirements for no excessive data collection, storage only as long as necessary, anonymity
- No right of effective personal appeal to a public body
- Onward transfer based on data protection agreement signed by third party

1.4 Need for Privacy-Enhancing Technologies for:

- Protecting the User-Identities providing *Anonymity*, *Pseudonymity*, *Unlinkability*, *Unobservability* of users
- Protecting Usee-Identities providing *Anonymity*, *Pseudonymity* of data subjects
- Protecting *Confidentiality* and *Integrity* of personal data

“Law Becomes Code Becomes Law”

Example: German Federal Information and Communication Services Act (TDDSG):

§3 (4) TDDSG:

The design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible

§ 4 (1) TDDSG:

The provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed about these options

§ 4 (4) TDDSG:

User profiles are permissible under the condition that pseudonyms are used. Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym