Organisation

• Teachers
  – Merel Koning (m.koning@cs.ru.nl)
  – Jaap-Henk Hoepman (jhh@cs.ru.nl)
• Blackboard is not used
  – Website: www.cs.ru.nl/~jhh/secsem.html

What is a seminar?

• Seminar
  – Student lecture
  – Student paper
  – Student opposition
• Grade = weighted average
  – But only if all grades are at least 5.5
  – If not, lowest grade is final grade!
• Working in groups
• Attendance required

Preliminary Course schedule
Topics

• First come first serve:
  – location privacy
  – Internet of things
  – identity management
  – electronic voting
  – smart metering/smart grids
  – Search/data retrieval
  – anonymous messaging
  – privacy in big data
  – Anonymous crypto currencies
    → your own...
• Sign up next lecture

Research

• analyse a particular practical case
  – what are the privacy issues (from a societal and legal perspective) and how are they dealt with
• give a precise and concise problem description
  – in technical terms: define your model; your assumptions
• investigate possible PETs that apply
  – summarise your analysis
• pick one and solve the problem (involves a protocol)
  – describe this in sufficient detail!
• (informally) prove or argue correctness

Student lecture

• Goal of lecture
  – to inform other students about your research
• Important
  – make lecture interactive
  – add additional material
• Discuss draft
  – Thursday 13:00-13:15 the week before
  – mail slides etc. at least 24 hours before

Student lecture: grading

• Content
  – Argumentation
    ∙ whether your lecture provides a solid basis and backing of all statements and claims made.
  – Cohesiveness
    ∙ whether the relationship between the different (sub)topics of your lecture is made clear.
  – Comprehensiveness
    ∙ whether your lecture covers all important aspects, and clearly separates important issues from secondary details. Equal attention should be paid to technical and legal/societal issues.
• Form
  – Structure
    ∙ logical ordering of your lecture, and its intelligibility.
  – AKrakveness
    ∙ audience captures the audience, and whether the message comes across (i.e. whether your lecture connects to what your audience expects and understands).
• Performance
  – Interaction
    ∙ level of engagement and contact with the audience, level of interactivity, the way you respond to questions.
  – Lecture technique
    ∙ your eye contact (comprehensibility), your presence in front of the class, your usage of supporting materials (e.g. powerpoint). The liveliness and tone of your lecture.
Student paper

- Goal
  - Report on research
  - Express own perspective on PETs
- Format
  - Roughly 10 pages (excluding references)
  - A4, reasonable margins, 10-11 pt font
- Beware
  - Find and use your own literature
  - Use input obtained during presentation in class

Student paper

- Typical structure
  - Context
  - Problem description
    - Including legal/social analysis
  - Proposed solution
  - Technical analysis
  - Conclusions

Student paper: planning

- Average timespan
  - Literature study: 2 weeks
  - Perform research: 2 weeks
  - Write skeleton: 1 week
  - Write final paper: 3 weeks
- Deadlines
  - May 3: Skeleton
  - June 14: Final paper
- So start April 1 at the latest

Student paper: grading

- Content
  - Technical quality
    - Whether the paper shows an understanding of the technical issues involved, correctness of all technical statements and claims, sufficient level of technical detail
  - Analysis
    - Whether a proper segmentation is given, and whether all main aspects of the topic are addressed, with proper regard of what are the main points and what are secondary points (this covers the criteria structure, coherence and comprehensiveness used for scoring the presentation)
  - Quality of references
    - Whether you found and cited all relevant literature, originality (finding relevant references yourself is appreciated)
  - Own opinion
    - Whether the paper clearly expresses and argues your own opinions on the subject matter
- Form
  - Style
    - Clarity of writing, objectivity, linguistic quality (in terms of spelling and grammar)
  - Structure
    - Logical structure of the paper, helping the reader understand what he is about to read, giving the paper a natural flow
  - Attractiveness
    - Formatting of the paper, including precise formatting of the bibliography
Remaining points

- Contribute to the wiki
  - http://wiki.science.ru.nl/privacy/

What is privacy?

Government surveillance
Commercial surveillance

Facebook and you
If you're not paying for it, you're not the customer. You're the product being sold.

Predictions

Shopping mall tracking (I call it Mallware)

Privacy

what is privacy according to you?
VALUES/GOODS/ENDS of privacy

- Personal value privacy e.g. Self-expression, Good Reputation, Repose, Intimacy and Formality, Human Dignity, Autonomy, Individualism
- Societal value privacy e.g. Limited Government, Toleration, Civility
- Both e.g. Intellectual Life, Preferences and Traditions

VALUES/GOODS/ENDS of privacy limitations


Privacy assets

- Personal data
- Home
- Reputation
- Information
- Body
- Etc..

Privacy threats

E.g. Threats to information privacy:

- Information Collection
  - Surveillance
  - Interrogation
- Information Processing
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion
- Information Dissemination
  - Breach of Confidentiality
  - Disclosure
  - Exposure
  - Increased Accessibility
  - Blackmail
  - Appropriation
  - Distortion
- Invasion
  - Intrusion
  - Decisional Interference
Collect > Process > Disseminate

Invasion/Use
Intrusion
Interference

Surveillance
Interrogation

Aggregation
Identification
Insecurity
Secondary Use
Exclusion

Breach of confidentiality
Disclosure
Exposure
Increased availability
Blackmail
Appropriation
Distortion

Definitions of privacy

Brandeis Warren 1890

- Privacy is ‘the right to be let alone’.
- ‘Hiding’

Westin 1968

- Privacy is ‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’.
- ‘Control’
Agre and Rotenberg 1998

- Privacy is ‘the freedom from unreasonable constraints on the construction of one’s own identity’.
- ‘Dialogue’

Nissenbaum 2004

- Contextual integrity: the right to prevent information to flow from one context to another
  – [Nissenbaum, 2004]

Contextual integrity

Don’t confuse these concepts!

security

privacy

data protection
Typologies and taxonomies

Privacy and identity theory

Allan Westin’s 4 privacy states

- 1960
- Privacy is linked to the needs of an individual
- Classification derived from case law on privacy torts (US)
  - Solitude: Most complete state of privacy: Individual separated from others
  - Intimacy: Beyond intimate relations. State of intimacy prerequisite for close contact
  - Anonymity: Public privacy. Freedom from identification and surveillance. Public spaces and anonymous publication
  - Reserve: Dynamic aspect of privacy in daily interpersonal relations. Psychological barrier against unwanted intrusions

Finn, Wright, Friedewald’s types of privacy

- 2013
- EU data protection legislation analysis
- Expanded from Clarke
- Bio-informatics, drones etc.

Finn, Wright, Friedewald’s

- Privacy of the person
- Privacy of behavior and action
- Privacy of communication
- Privacy of data and image
- Privacy of thoughts and feelings
- Privacy of location and space
- Privacy of association
RFID-enabled travel documents

- **Assets:**
  - Information on the chip itself:
    - Travel routes
    - Frequent destinations
    - Rare destinations
    - Mode of transport.
  - Information in the database:
    - Location time
    - Possible co-travelers etc.
    - Routes
    - Identity

- **Threats:**
  - Data collection
    - Surveillance
    - Interrogation when card is issued or when error occurs
  - Processing
    - Secondary use
    - Aggregation
    - Insecurity
  - Dissemination
    - Disclosure and exposure
    - Invasion
    - Decisions on identification

Second generation biometrics

- **Measurement and analysis of biometric traits:** gait analysis, voice recognition
- **Psychological biometric:** pheromone detection, heartbeat analysis, bodyheat etc.

- **Impact all seven types**
Privacy

- Computing (1950-)
  - Searching becomes efficient
  - Data kept forever

- Networking (1980-)
  - Data sharing becomes easy
  - Data accessible online

"network effect"

Different types of data/information

- Volunteered
  - What you reveal explicitly when asked
- Observed
  - What you reveal implicitly by your behaviour
- Inferred
  - What is derived from other data about you

[World Economic Forum Report Personal Data: The Emergence of a New Asset Class]

Data vs Metadata

- Metadata (= Behavioural data)
  - Condensed (information rich, easy to process)
  - More "true" (judge a man not on what he says but on what he does)

Why is privacy important
“Privacy is essential for freedom, democracy, psychological well-being, individuality and creativity”


Moral basis for data protection

- prevention of information-based harm
  - Like guns, information may kill people
- prevention of informational inequality
  - The “market” of information
  - Non-discrimination
- prevention of informational injustice
  - Spheres of privacy must be protected
- respect for moral autonomy.
  - People change


Searching for the right metaphor

Huxley / Brave New World
Nineteen Eighty-Four / Orwell
The Man In The High Castle / Philip K. Dick
The Matrix / Larry Wachowski
The Social Dilemma / Jaron Lanier

Of:

- Big Brother / George Orwell
- Little Sister / Chandler
- The Trial / Franz Kafka
You’ve got nothing to hide

Everybody has something to be embarrassed about

Assumes that the problem is data you want to hide — even “innocent” data can harm you

Freedom of thought

— That job offer looks interesting...
— That woman looks “interesting”...

No distinction between illegal (legal) vs disgraceful (moral) vs ...

What is the data used for: investigation, anti-terrorism, or ...

Function creep

Wrong assumption

The point is not that there is data that is apriori “wrong” or illegal (as seen by the “sender”)

The point is that “innocent” data can (later) be used wrongly (by the current “receiver”)


Beyond privacy: autonomy
Resources

• Websites
  – http://wiki.science.ru.nl/privacy/
  – https://www.eff.org/

• Books
  – Ilija Trojanow, Juli Zeh "Aanslag op de vrijheid", de Geus, 2010