Privacy - Introduction

Dr. Anne Kayem

Email: anne.kayem@guest.hpi.de / anne.kayem@hpi.uni-potsdam.de

Today…

- Title: “Privacy – Algorithmic Foundations and Usability“
- General Course Structure
  - Portfolio (50%), Presentations (30%), Final Exam (20%)
- Overview and Goals / Learning Objectives
- Challenges in Quantifying Privacy and Usability
  - What does privacy mean to you?
  - Privacy Goals
  - Why Privacy is hard to measure?
  - How Privacy is protected?
  - Privacy notice and choice

General Structure

- 14 Meetings (25.04 – 25.07)

- Block 1: 6 Lectures (Background Material)
  - Topic Choice: Doodle Poll (see course description)
  - Topic Assignment (Week 4: 16.05)

- Block 2: 6 Meetings (Portfolio and Presentation)
  - Meeting 1 (06.06): Project Proposal (one page)
  - Meeting 2 (13.06): User Consent Form
  - Meeting 3 (20.06): Questionnaires, Scripts, Scenarios
  - Meeting 4 (27.06): Prototypes for User Studies
  - Meeting 5 (04.07): 5-10 min progress report
  - Meeting 6 (11.07): Discussion – User Studies

General Structure

- Block 3: Evaluations
  - Final Presentations (18.07): 15 – 20 min slots
    - (Doodle poll to decide date – mid May??)
  - Portfolio Handin (15.08)
  - Final Exam (25.07): Open Book / Oral
    - (Doodle poll to decide date – early June??)
  - Course material available Online

Interest in Publication?

- Some Options… (speak to me about …)
  - PASSWORDS 2017 (Deadline: August 2017)
  - PETS 2018 (Deadline: August/November 2018)
  - ICDE 2018 (Deadline: October 2017)
  - CHI 2018 (Deadline: November 2017)
  - SOUPS 2018 (Deadline: March 2018)

Personal Data Collection…

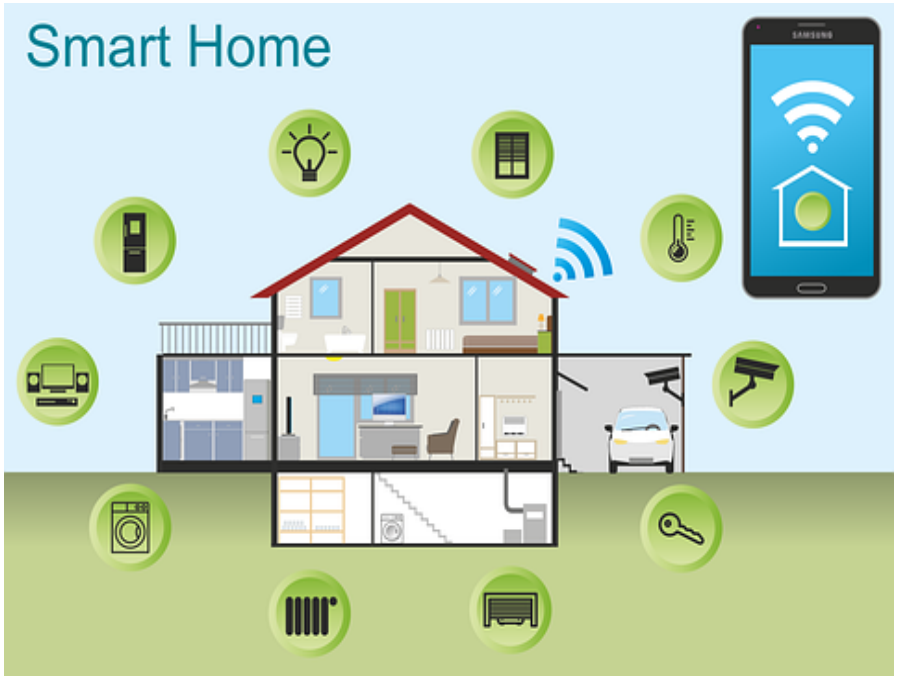
- Large amounts of personal data are collected daily
  - Governments, Private Entities, … (various sources)
  - 500 million tweets on Twitter
  - 350 million photographs on Facebook

Privacy Loopholes (Example)…

- Case #1: Geo-location Data
  - https://iapp.org/news/a/the-next-privacy-frontier-geolocation/
  - Knowledge of the location of a device within a given time period can be used to uniquely identify the location history of the device (95%)

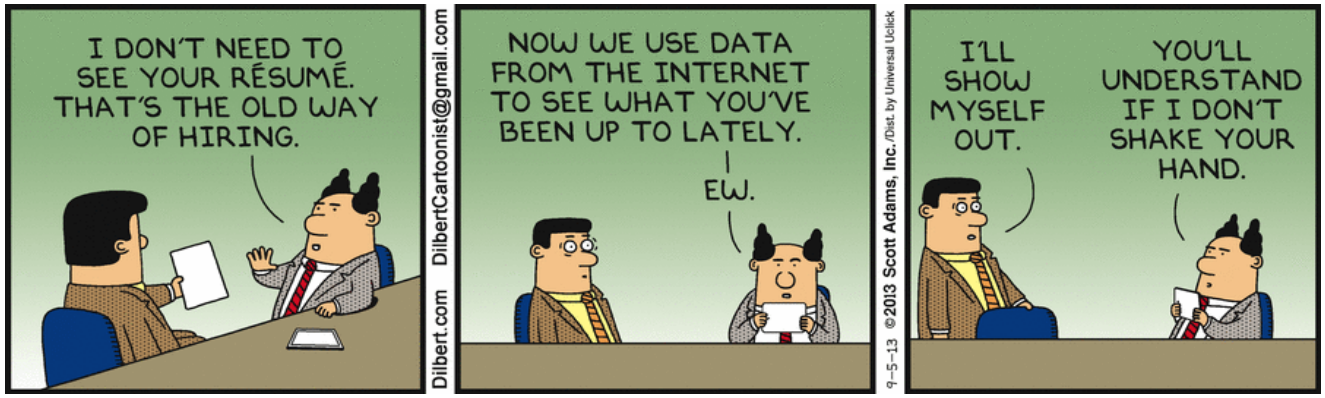
Privacy Loopholes (Example)…

- Case #2: CIA Surveillance
  - Hacking into phones, smart TVs, and computers
  - Across the world
  - Unconfirmed by CIA (but questions privacy)
  - https://www.cnet.com/news/un-privacy-expert-slams-global-digital-internet-surveillance/



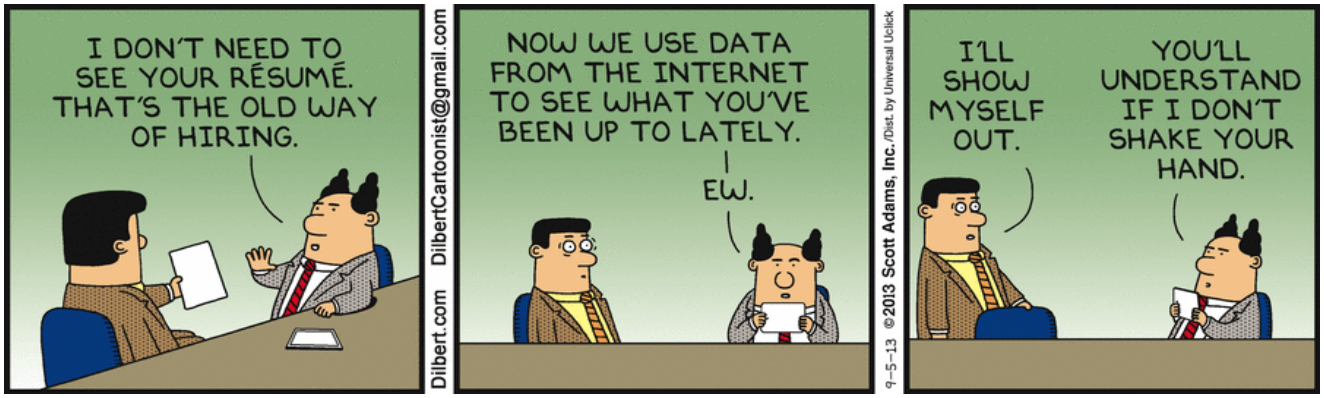
Privacy

What does privacy mean to you?



Privacy and What it means…

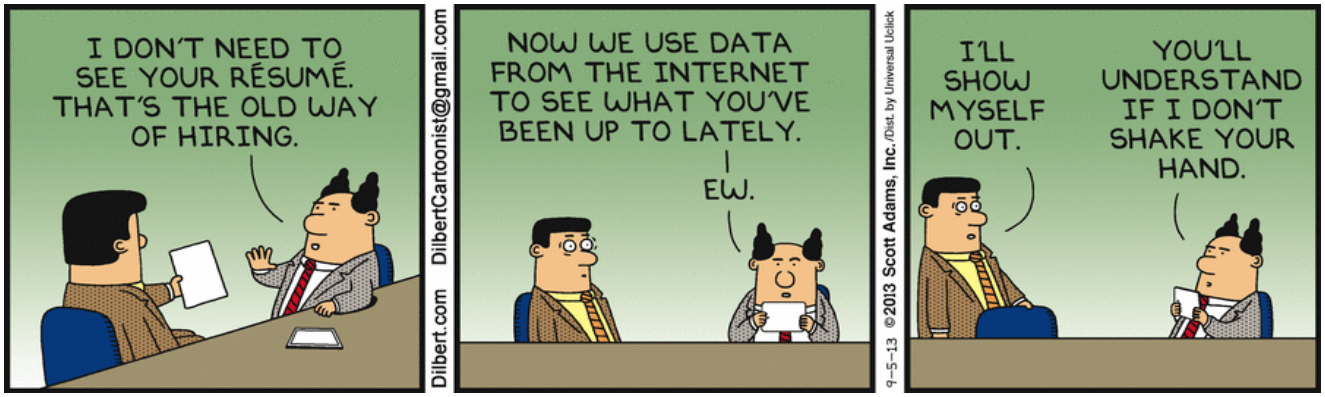
- Hard to define … („Three Concepts of Privacy", R.C. Post)



- Complex (what are my rights, information veracity?...)
- Contradictory (People lie on resumes …)
- Conflicting objectives (Data Analytics is useful…)

Privacy and What it means…

- Information Control…



"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…"

Privacy Goals…

What I want …	What I want to be …
Not misjudged	Identity
Solitude	Not required to reveal
Not profiled	Unknown
Not targeted	Forgotten
Free to try/make errors	Safety
Not talked about	Control
Unseen, unheard,…	Boundaries

Measuring Privacy…

- Why is privacy hard to measure?
- Why are attitudes about privacy hard to measure?
- Why is the cost of privacy invasion hard to measure?

How is Privacy Protected…

- Laws, self regulation, technology
  - Notice and access
  - Control over collection, use, deletion, sharing
  - Collection limitation
  - Use limitation
  - Security and accountability

Privacy Laws…

- Vary from country to country

- Example: The US has no explicit constitutional right to privacy or general privacy law
- (Most privacy rights are inferred from the constitution)

- EU Data Protection Directive
  - Comprehensive Laws
  - Privacy as a fundamental human right
  - Privacy commissions in each country

OECD Fair Information Principles…

- OECD: Organisation for Economic Co-operation & Development

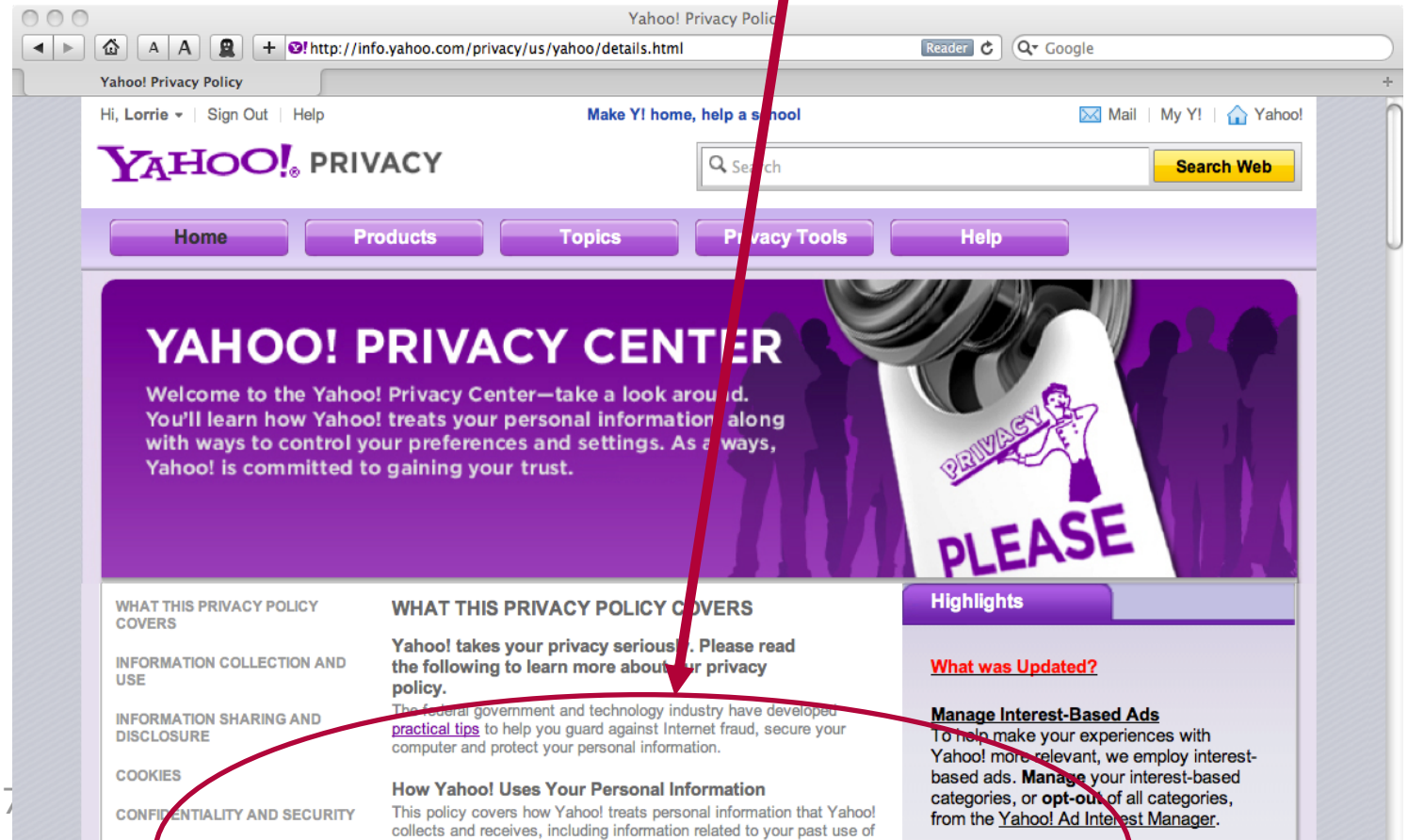
- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openess
- Individual Participation
- Accountability

- https://www.privacyrights.org/ar/fairinfo.htm

Notice and choice…

- Protect privacy by giving people control over their data

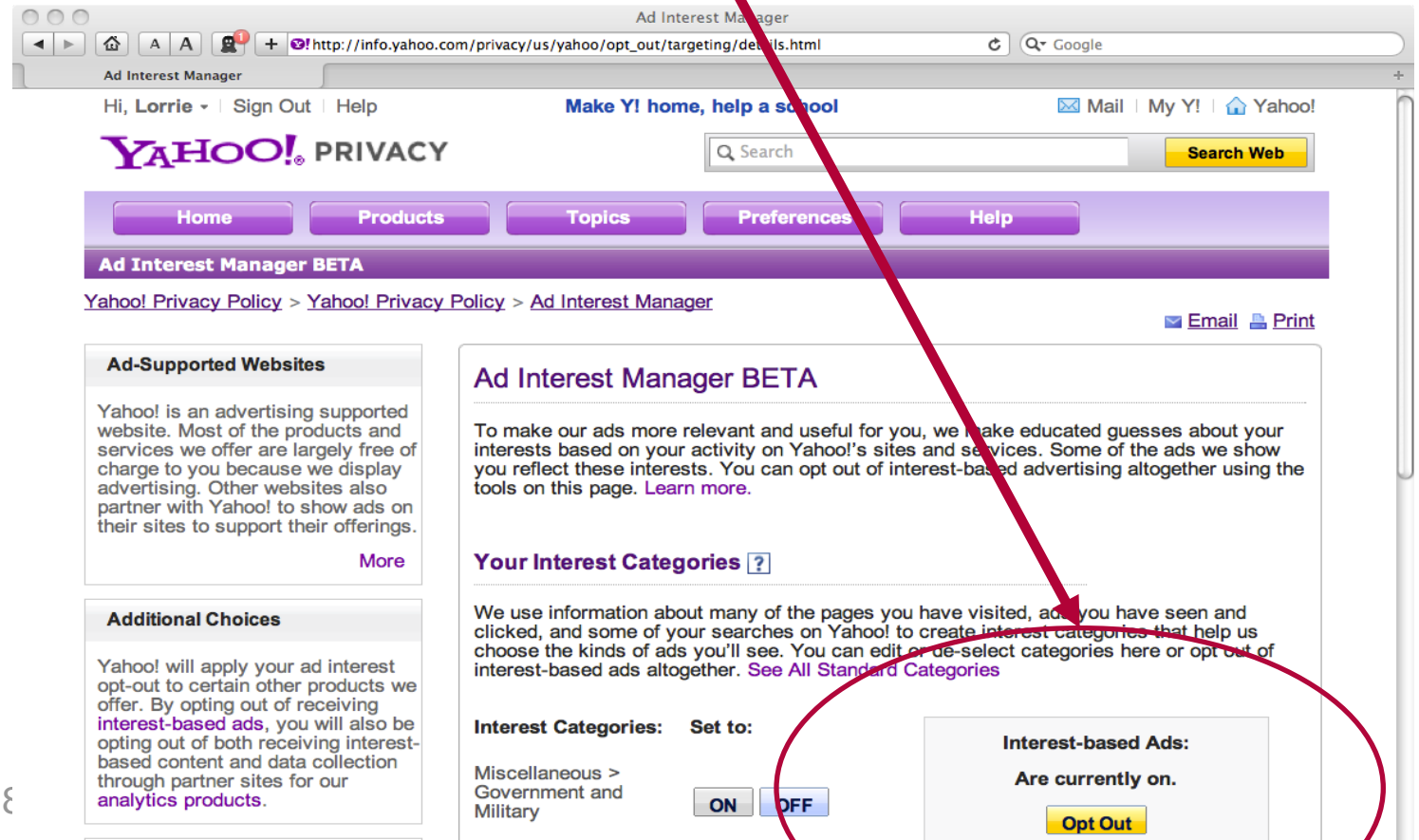
Notice about data collection and use



Notice and choice…

- Protect privacy by giving people control over their data

Choices about data collection and use in specific ways



Reading Privacy Policies…

- Notice and choice model (Privacy Enforcement)

- Implemented in the form of long, incomprehensible privacy policies that consumers typically do not read, and are difficult to understand”

- Can we learn from the food processing industry?

Privacy Icons ...

- https://www.fastcodesign.com/1662961/mozillas-privacy-icons-tell-you-how-sites-use-your-personal-data

Your data is never bartered or sold.

Your data may be bartered or sold.

Your data is kept for less than 1 month.

Your data may be kept indefinitely.

Next Week…

- Authentication – Privacy and Usability Considerations
  - Passwords
  - Identity Leak Checker (pros and cons: usability-wise)
- Reading Material Available Online

Think About…

- Observe people in a public place who are using a computer system.
- Try to work in pairs (or do this with a friend)
- **Example:** People using a public transit ticket machine, a library self-checkout machine, or an airport self-check-in kiosk.
- Stay long enough to observe both experienced and inexperienced users using the system.

Think About…

- Make some notes about your observations.

- **Examples:**

1. What problems did people have using the system?
2. What seemed easy to learn? Why?
3. What was difficult to learn/understand?
4. What seemed to frustrate experienced users?
5. How might the design of the system be improved?