University of Kent

Computing

CO643 – Week 9
Usable Computing

Dr Özgür Kafalı

Lecturer

R.O.Kafali@kent.ac.uk

Outline

- Usable security warnings/nudges
- Usable privacy policies and notices
- US vs UK/EU laws concerning privacy
- Privacy attitudes
- Cultural studies

Learning Outcomes

- After this lecture, you will be able to
  - Describe various usable security/privacy solutions
  - Evaluate usable privacy policies
  - Compare privacy laws for different countries
  - Understand how people react to privacy in different cultures

How the Camera Doomed Google Glass

http://www.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions/index.html
https://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570/

Utility vs Privacy

Koppel et al. Workarounds to computer access in healthcare organizations: You want my password or a dead patient? Studies in Health Technology and Informatics, 208:215-220, 2015

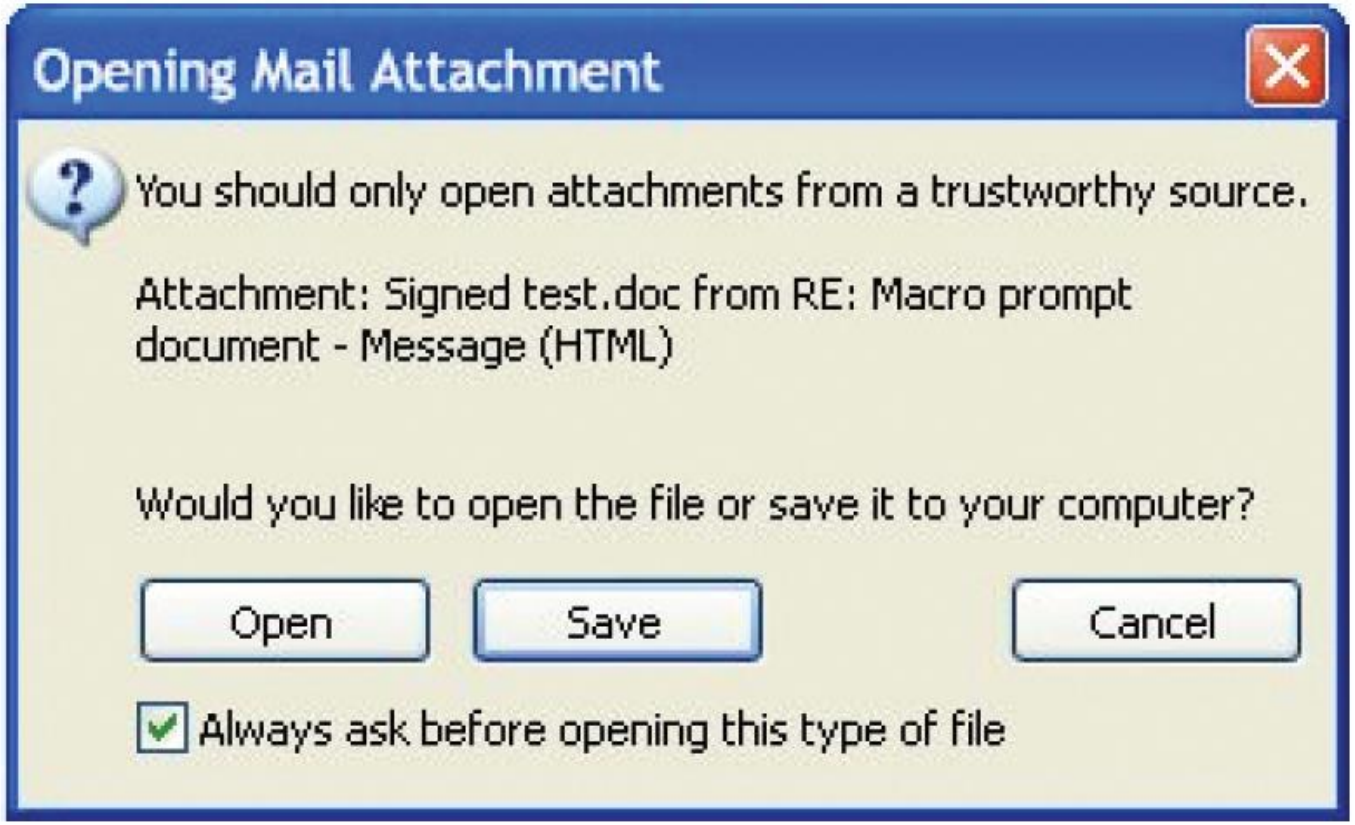
Privacy Engineering

- Integrating privacy solutions into everyday engineering practices
- Data protection requirements
- Beyond data breaches: Perceptions matter too

Bounded Rationality

- Even if complete information is available, hard to process such data
- <u>Survey question:</u>
  - You completed a credit card purchase with an online merchant
  - Besides you and the merchant, who else has data about parts of your transaction?

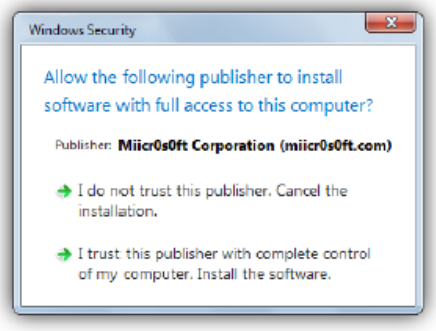
Usable Warnings



Bravo-Lillo et al. Bridging the gap in computer security warnings: A mental model approach
IEEE Security and Privacy, 9(2):18-26, 2011

Example Warning

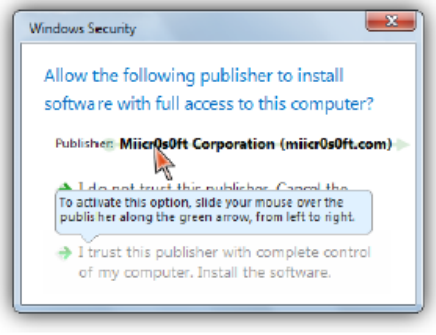
Variations



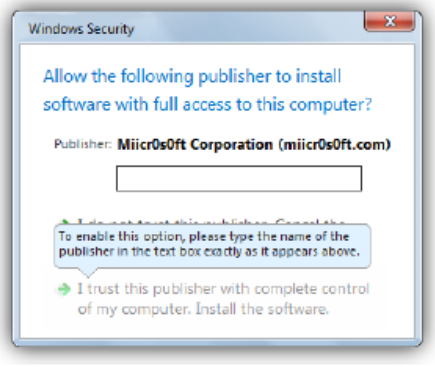
(a) *Control*

(b) *Animated Connector (AC)*

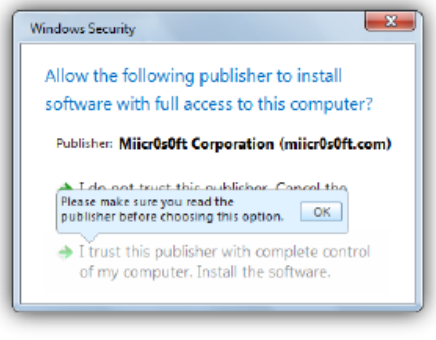
(c) *Progressive Reveal*



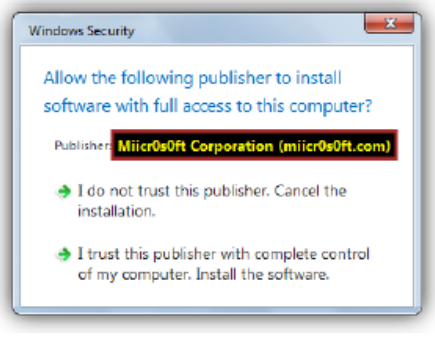
(d) *Swipe*



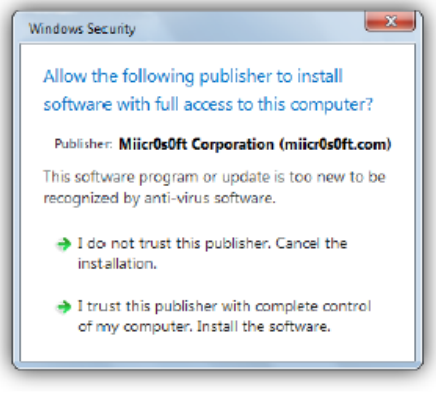
(e) *Type*



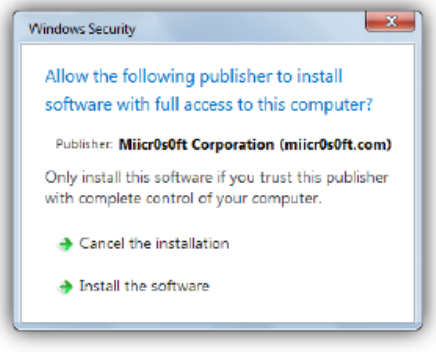
(f) *Request*



(g) *ANSI*



(h) *No Antivirus*



(i) *Short options*

Advanced vs Novice Users

- Novice users assess an action after seeing its consequences
- Advanced users judge an action a priori
  - Look for vulnerabilities in public forums
  - Regularly patching software
  - Typing URLs directly rather than clicking a link

Nudges

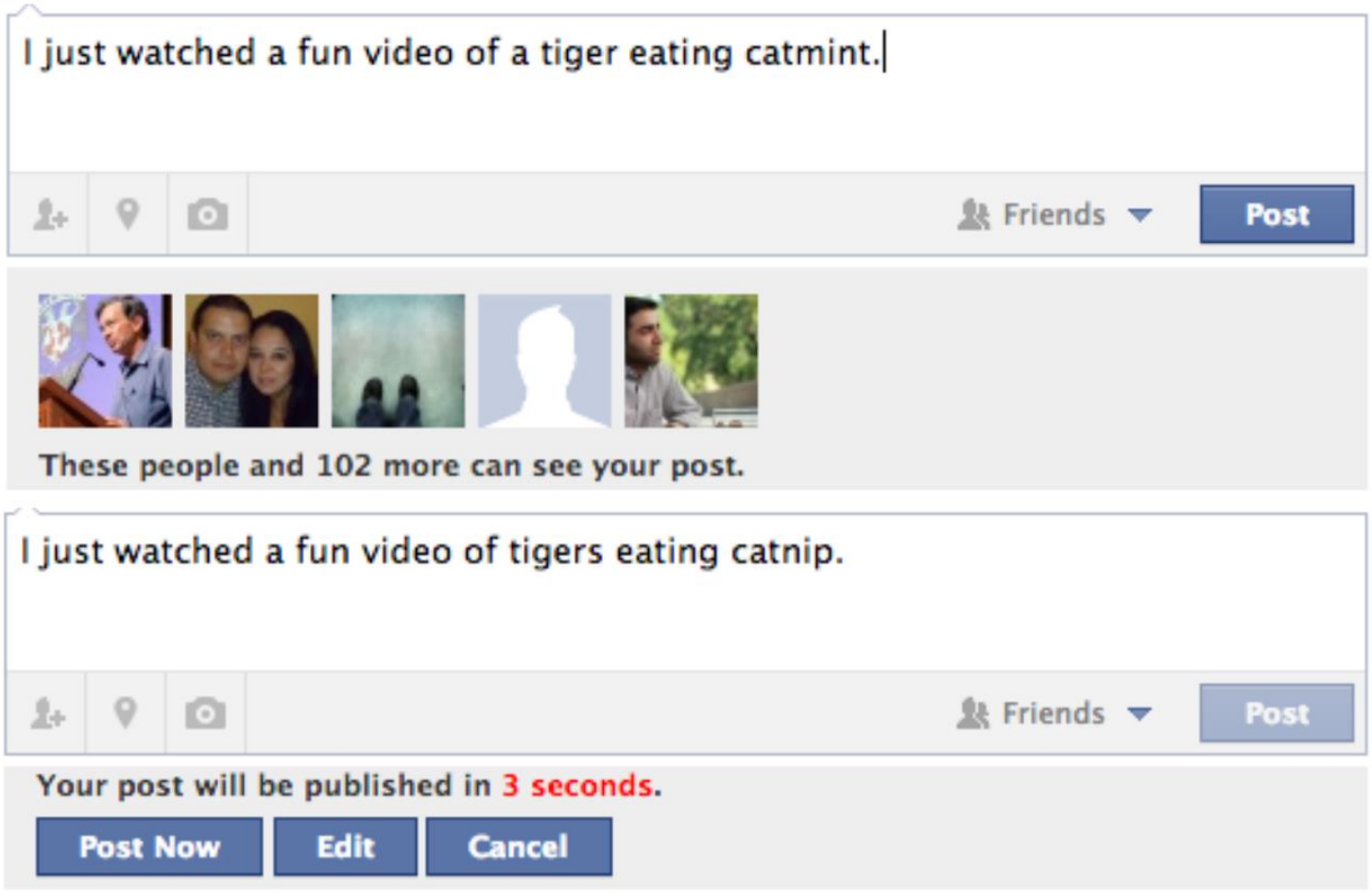
- Multi-disciplinary research to assist users with privacy decision-making
  - Human computer interaction
  - Persuasive technology
- Example: Create stronger passwords - Password strength meter

Privacy Nudges for Facebook

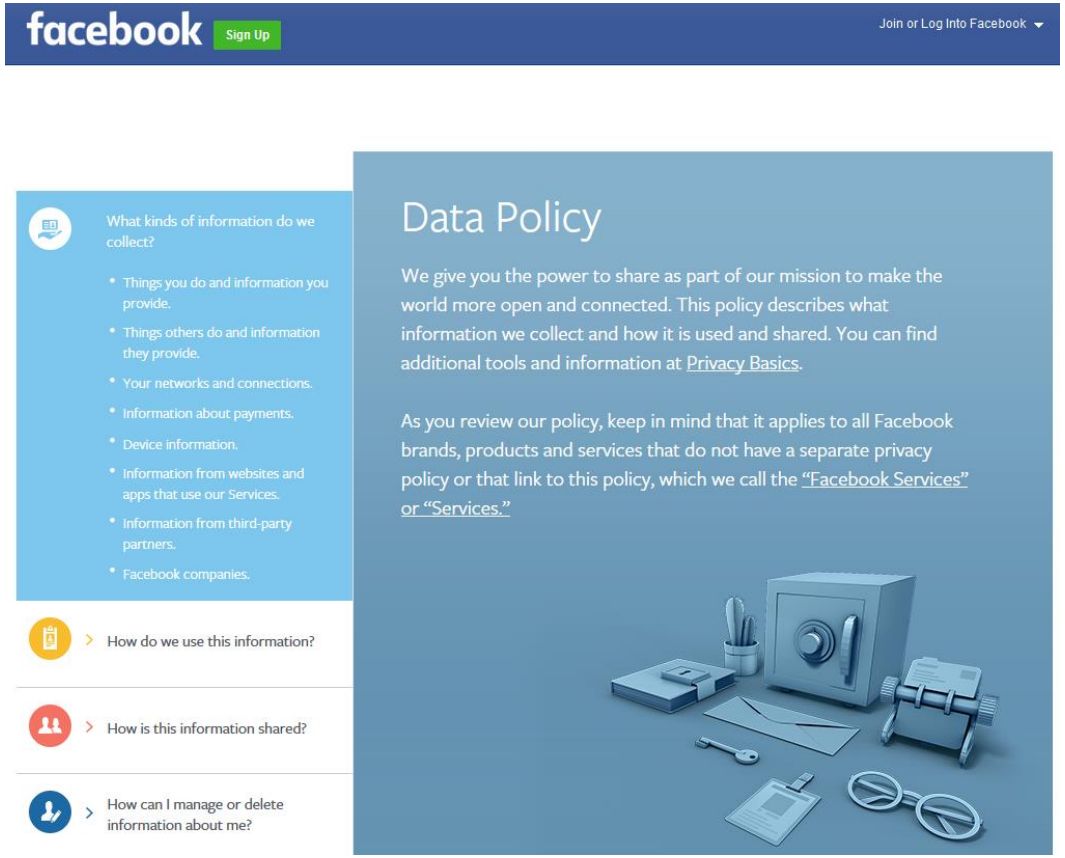
- Audience nudge: Remind users about the audience for their post
- Timer nudge: Make users pause and think before posting

Wang et al. A Field Trial of Privacy Nudges for Facebook
Conference on Human Factors in Computing Systems, pages 2367-2376, 2014

Audience & Timer



Privacy Policies



Facebook privacy policy is longer than the US constitution

http://www.huffingtonpost.com/2010/05/12/facebook-privacy-policy-s_n_574389.html

University of Kent

Computing

Nutrition Labels

Kelley et al. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach
Conference on Human Factors in Computing Systems, pages 1573-1582, 2010

Standardized Tables

Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
preferences		opt out	opt out			
purchasing information		opt out	opt out			
your activity on this site		opt out	opt out			

Information not collected or used by this site: social security number & government ID, financial, health, location.

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

	we **will** collect and use your information in this way		we **will not** collect and use your information in this way
opt out	by default, we **will** collect and use your information in this way unless you tell us not to by opting out	opt in	by default, we **will not** collect and use your information in this way unless you allow us to by opting in

Privacy Notices

- Purpose: Make users aware of data practices involving personal information
- Privacy notice: Public announcement of data practices regarding
  - Collection
  - Usage
  - Sharing

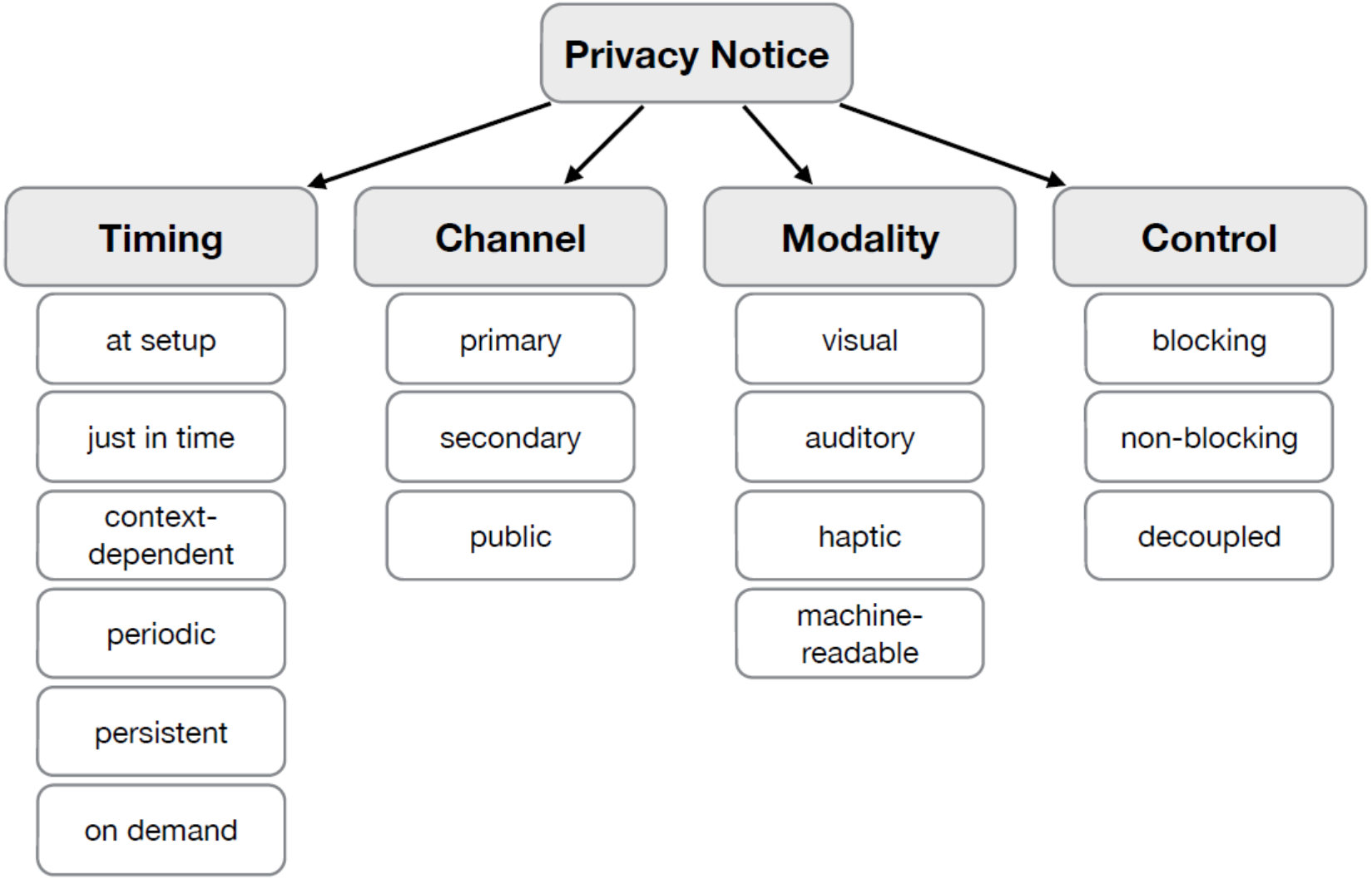
Schaub et al. A Design Space for Effective Privacy Notices
Symposium On Usable Privacy and Security (SOUPS), 2015

Challenges

- Notice complexity: 244 hours annually to read all policies for websites visited
- Lack of choices: Informative, but not actionable "Warning: CCTV in use"
- Notice fatigue: Often shown at inopportune times, conflict with user's main task
- Decoupled notices: For example, a fitness tracking device

Schaub et al. A Design Space for Effective Privacy Notices
Symposium On Usable Privacy and Security (SOUPS), 2015

Design Space



Schaub et al. A Design Space for Effective Privacy Notices
Symposium On Usable Privacy and Security (SOUPS), 2015

Privacy Laws: EU

- New General Data Protection Regulation (GDPR - May 2018) replaces EU Data Protection Directive 95/46/EC (late 90s)
- Objective:
  - Not only protect EU citizens' sensitive data
  - But also enable them to manage their data in a more controlled way

Privacy Laws: US

- Different approach
- No single regulation, but rather sector based
  - Health Insurance Portability and Accountability Act (HIPAA)
  - National Institute of Standards and Technology (NIST)
  - Federal Trade Commission (FTC)
  - Financial institutions (Gramm-Leach-Bliley Act)
  - Federal agencies

GDPR

- Every individual located within the EU must be guaranteed the same rights and freedoms
- More focus on individual rights than the interests of businesses
- Not only apply to organisations based within the EU, but to any organisation that processes EU citizens' data

GDPR Main Changes

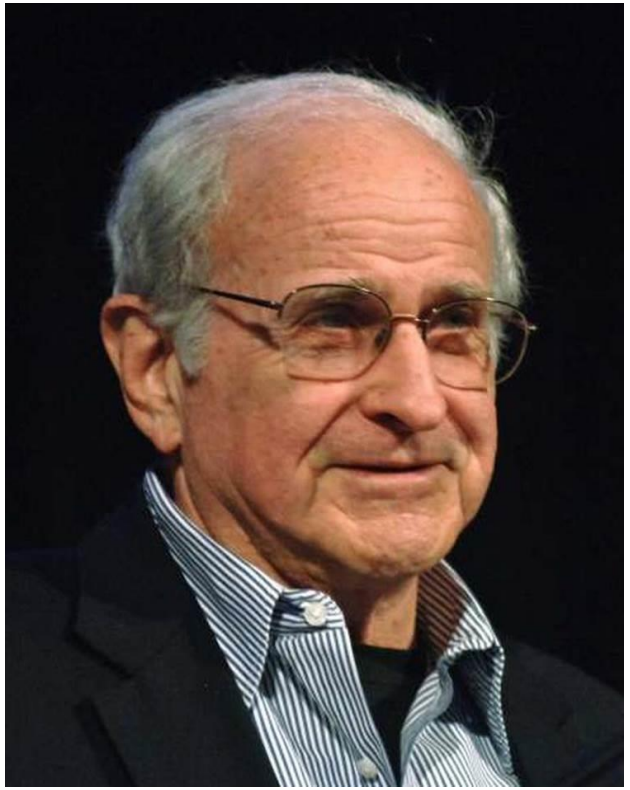
- Increased territorial scope
- Penalties
- Consent
- Data subject rights

https://eugdpr.org/the-regulation/

Differences: US vs EU

- Breach notification
- Right to be forgotten
- Freedom of information request
- Protection of children’s data

Privacy Categories



- Alan Westin half a century ago defined the modern right to privacy before the Web era
- Three categories:
  - Fundamentalist
  - Pragmatist
  - Unconcerned

Westin. Privacy and Freedom. New York: Atheneum, 1967

Westin Privacy Index

- Classify the public into three categories
- Fundamentalist (25% of Americans): Distrustful of organizations, refuses to give out personal information
- Pragmatist (55% of Americans): Weighs the value of consumer opportunities, aware of privacy risks
- Unconcerned (20% of Americans): Does not know what the "privacy fuss" is about

Westin's Original Survey

1. Consumers have lost all control over how personal information is collected and used by companies
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way
3. Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today

Fundamentalist

- Fundamentalists are generally distrustful of organizations that ask for their personal information, worried about the accuracy of computerized information and additional uses made of it, and are in favor of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies. They generally choose privacy controls over consumer-service benefits when these compete with each other.

Pragmatist

- They weigh the benefits to them of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved. They look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved. They believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it. And, where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists.

Unconcerned

- The Unconcerned are generally trustful of organizations collecting their personal information, comfortable with existing organizational procedures and uses are ready to forego privacy claims to secure consumer-service benefits or public-order values and not in favor of the enactment of new privacy laws or regulations.

Applicability of Westin's Survey

- Conduct human subject research on privacy
- Compare reported behavior vs actual privacy related actions
- Organisations might use this data to target pragmatists
- Provides insights for organisations to respond to privacy concerns with appropriate policies, products, and services

Follow-up Studies

- A marketing company offers you $1000 and free genetic testing in exchange for the rights to all your current and future medical records. They will have the right to resell or publish your data (anonymously or with information that could identify you, at their discretion).
- Main question: How likely would you be to take the offer?

Woodruff et al. Would a Privacy Fundamentalist Sell Their DNA for $1000... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. Symposium on Usable Privacy and Security (SOUPS), pages 1-18, 2014

Alternative Outcomes

- Outcome 1: Your medical data is combined with that of many others. It is used to find a new cure for a previously deadly disease. Neither you nor anyone in your family has this disease.
- Outcome 2: Your data is published with information that identifies you. You lose a job due to your genetic information, which falsely suggests you may later develop a serious medical condition.

Alternative Outcomes

- Outcome 3: Your data is used to calculate the probability of certain diseases developing within your family. As a result, some of your relatives (but not you) see an increase of several hundred dollars a year in their health insurance premiums.
- Outcome 4: Your test results reveal that you have a serious but treatable disease of which you were previously unaware. You receive treatment just in time to make a full recovery.

Privacy Attitudes

- People
  - Mental models of humans for privacy decision making
- Cultures
  - What changes in privacy behaviour and attitudes among different cultures?
  - What factors cause such changes?

Us and Them

- Objective: Understand privacy expectations from modern software systems
- What are developers' and users' perceptions of privacy?
- Does experience in software development have any impact on privacy requirements?
- Does geography have any impact on privacy requirements?

Sheth et al. Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe International Conference on Software Engineering (ICSE), pages 859-870, 2014

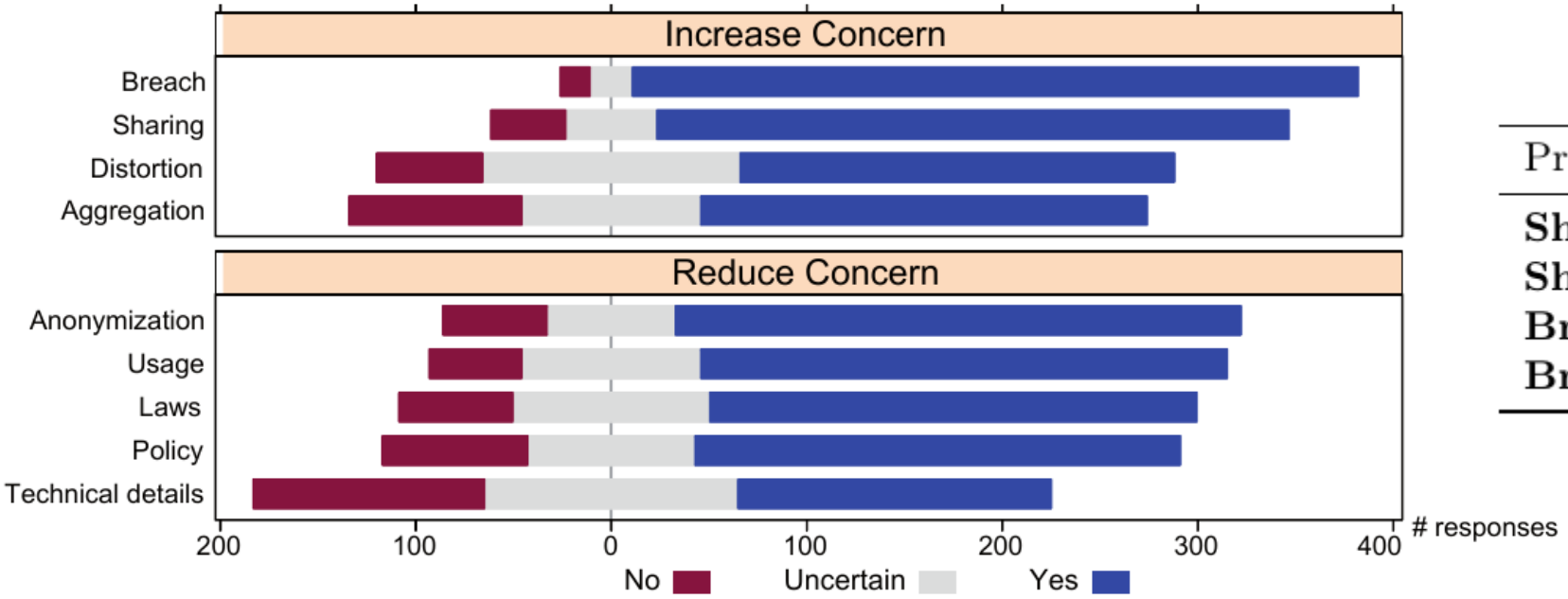
Factors to Increase Privacy Concerns

- Data aggregation: The system discovers additional information about the user by aggregating data over a long period of time
- Data distortion: The system might misrepresent the data or user intent
- Data sharing: The collected data might be given to third parties for purposes like advertising
- Data breaches: Malicious users might get access to sensitive data about other users

Factors to Reduce Privacy Concerns

- Privacy policy, license agreements: Describing what the system will/will not do with the data
- Privacy laws: Describing which national law the system is compliant with
- Anonymising all data: Ensuring that none of the data has any personal identifiers
- Technical details: Describing the algorithms/source code of the system in order to achieve higher trust (e.g. encryption of data)
- Details on usage: Describe in a “usable” table the uses of data

Perceptions



Privacy concerns	p-values
Sharing > Aggregation	$p = 1.231e^{-12}$
Sharing > Distortion	$p = 6.036e^{-14}$
Breach > Aggregation	$p < 2.2e^{-16}$
Breach > Distortion	$p < 2.2e^{-16}$

Sheth et al. Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe International Conference on Software Engineering (ICSE), pages 859-870, 2014

Giving up Privacy

- Would you accept less privacy for the following?
  - Monetary discounts
  - Added functionality of the system
  - Fewer ads
- 37% accepts less privacy for added functionality
- 21% accepts less privacy for monetary discounts
- 14% accepts less privacy for fewer ads

Role of Geography

- America thinks all types of data are less critical than Europe and Asia
- No statistically significant difference between Europe and Asia
- Added functionality: 51% of Europe does not give up, only 24% for America
- Europe feels that providing usage details is more effective than laws and policies
- America feels all options are equal

Components of Privacy Framework

- Anonymisation
- Data usage details
- Default encryption
- Fine-grained control
- Time and space limited storage
- Policies and laws

Mechanical Turk Workers vs US Public

- Crowd workers: Chosen an anonymous, flexible worksite
- Compared to the general population
  - Better educated
  - More liberal
  - Younger

Kang et al. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public
Symposium on Usable Privacy and Security (SOUPS), pages 37–49, 2014

University of Kent

Computing

Demographics

- US Public vs mTurk

Demographic Characteristics	U.S. Public	U.S. Turk	Indian Turk
N	**775**	**182**	**128**
Age			
18-24	12%	24%	23%
25-34	14%	41%	56%
35-44	13%	23%	12%
45-54	17%	9%	5%
55-64	24%	3%	2%
65+	19%	1%	2%
Mean age	49.8	32.7	30.5
	F [2,1080] = 122.72, $p < .001$		
Gender			
Female	50%	42%	35%
Male	50%	57%	65%
	X^2 [2, 1084] = 11.76, $p < .01$		
Education			
High school or less	26%	12%	5%
Some college	31%	45%	14%
College and more	42%	43%	81%
	F [2,1080] = 24.62, $p < .001$		
Percent who use social media	68%	90%	98%
	X^2 [2,1085] = 97.04, $p < .001$		

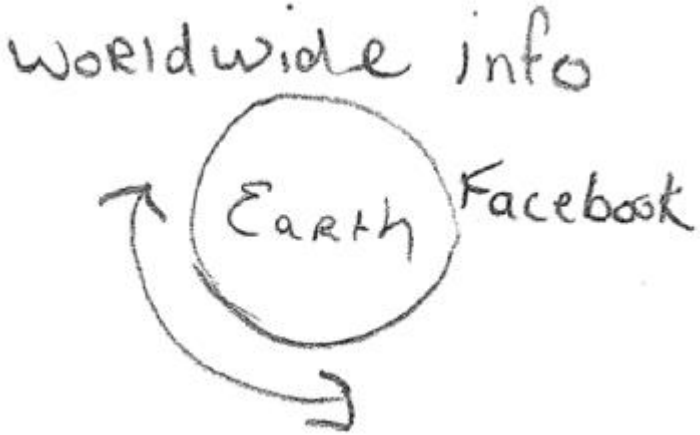
Kang et al. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public Symposium on Usable Privacy and Security (SOUPS), pages 37–49, 2014

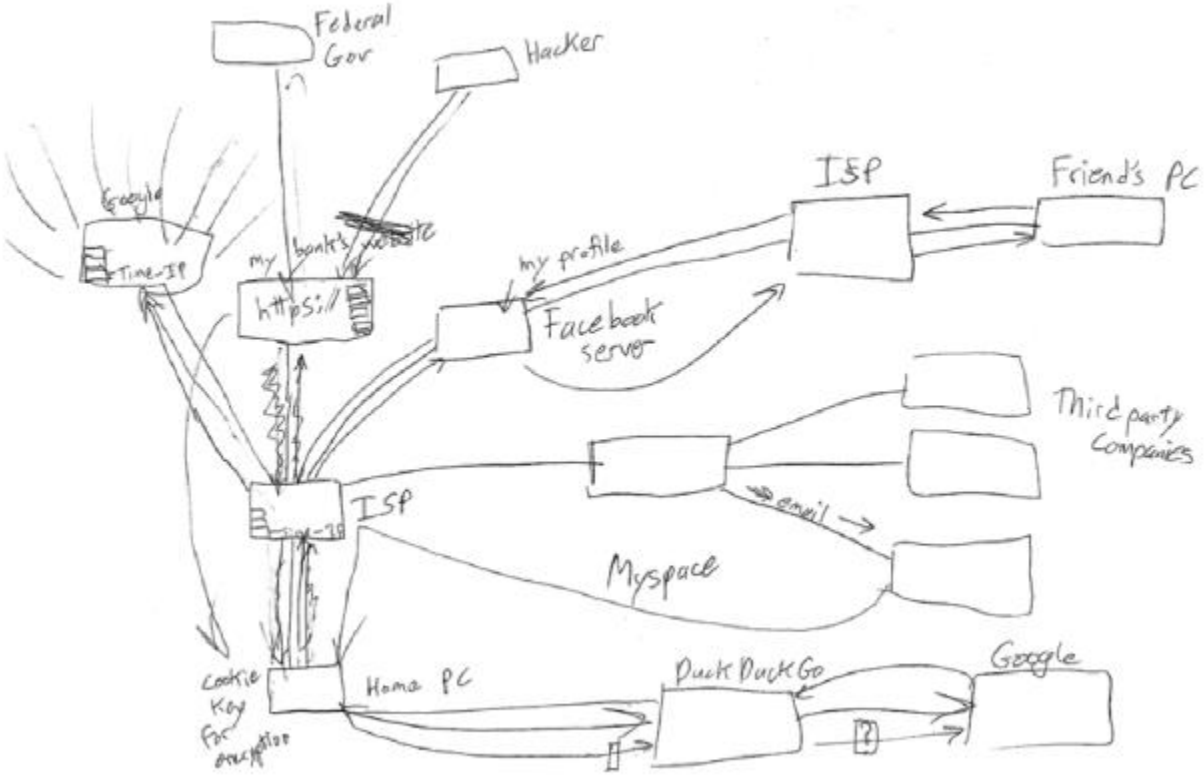
Knowledge of Internet

- Declarative knowledge: Knowledge about facts and terms (e.g. privacy settings, tagging, bcc)
- Procedural knowledge: How to take actions and complete tasks
- Technical familiarity
- Awareness of institutional practices
- Policy understanding
- User skills
- Awareness of security threats and tools

Kang et al. My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security Symposium On Usable Privacy and Security (SOUPS), pages 39-52, 2015

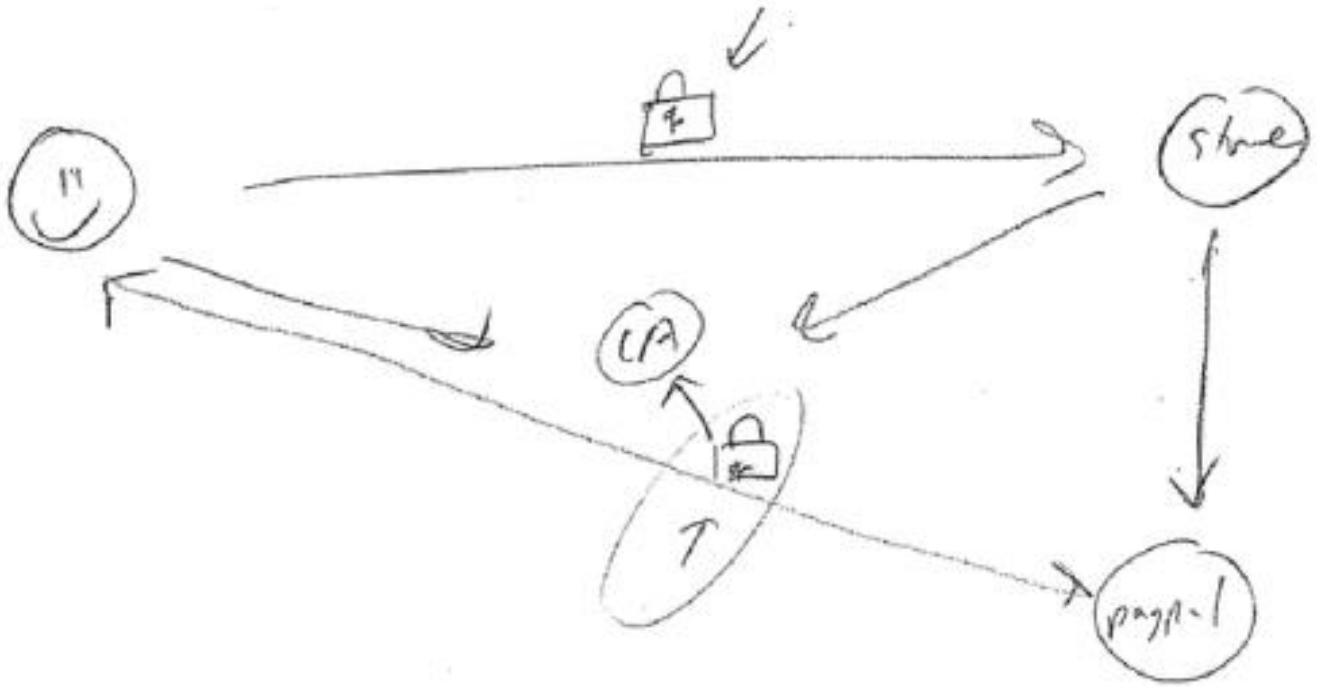
Who Can See My Data?





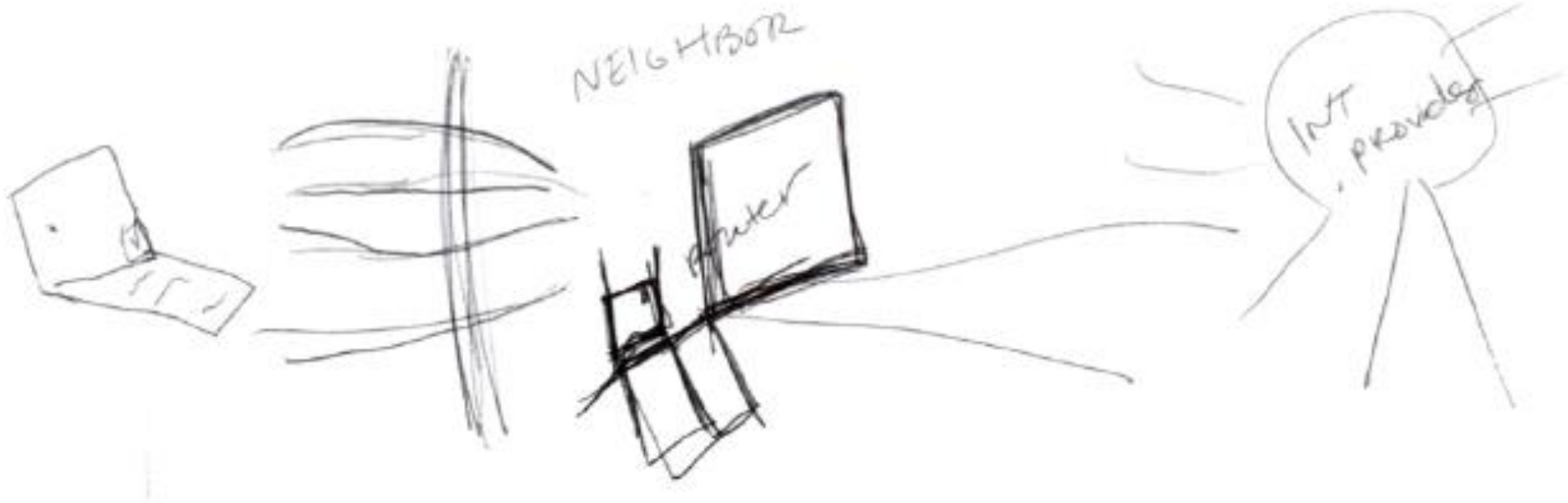
Kang et al. My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security Symposium On Usable Privacy and Security (SOUPS), pages 39-52, 2015

Making Online Payment to a Shoe Store



Kang et al. My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security Symposium On Usable Privacy and Security (SOUPS), pages 39-52, 2015

How to Use Neighbour's WiFi



Kang et al. My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security Symposium On Usable Privacy and Security (SOUPS), pages 39-52, 2015

Reasons for not Taking Privacy Actions

- I have nothing to hide
- Doing so would sacrifice effectiveness or convenience
- Poor usability of privacy protection tools
- Lack of procedural knowledge

Conclusions

- In this lecture, we have
  - Reviewed usable security/privacy solutions
  - Compared US and UK/EU laws for privacy
  - Seen how privacy attitudes can differ among people
  - Seen how privacy attitudes can differ among cultures

Additional Material

- Kumaraguru and Cranor. Privacy indexes: A survey of Westin's studies. 2005
- Kang et al. My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security. Symposium On Usable Privacy and Security, pages 39–52, 2015
- https://www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html
- TED talks:
  - https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd